

**ORGANISATIONAL INFORMATION SYSTEMS**  
**RESILIENCE : A Q-METHODOLOGY APPROACH**

---

A thesis submitted in partial fulfilment of the requirements for the Degree

of Master of Commerce (Hons) in Information Systems

in the University of Canterbury

by Amitrajit Sarkar

University of Canterbury

2016

---

INFO690

College of Business and Law



# Organisational Information Systems Resilience : A Q-Methodology Approach

## Master of Commerce (Hons) in Information Systems Thesis

*Semester 1, 2016*

*Department of Accounting and Information Systems*

**Postgraduate Student**

Amitrajit Sarkar

Department of Computing, Ara Institute of Canterbury Phone 940 8495

Email: [sarkara@cpit.ac.nz](mailto:sarkara@cpit.ac.nz)

**Senior Supervisor**

Dr. Stephen C Wingreen, Rm 419, Phone 364 2651, ext 6651

Email: [stephen.wingreen@canterbury.ac.nz](mailto:stephen.wingreen@canterbury.ac.nz)

**Co- Supervisor**

Trevor Nesbit, Brighton Business School; University of Brighton

Email: [T.Nesbit@brighton.ac.uk](mailto:T.Nesbit@brighton.ac.uk)

16

# TABLE OF CONTENTS

<i>Abstract</i>	<b>6</b>
<b>1. Introduction</b>	<b>12</b>
<b>2. Literature Review</b>	<b>16</b>
<b>2.1 Hazards and Threats</b>	<b>16</b>
<b>2.1.1 Natural threats</b>	<b>16</b>
<b>2.1.2 Technical threats</b>	<b>16</b>
<b>2.1.3 Human threats</b>	<b>17</b>
<b>2.2 Hazards in New Zealand Organisations</b>	<b>17</b>
<b>2.3 Resilience of Organisations</b>	<b>19</b>
<b>2.4 Importance of IS Resilience in Organisations</b>	<b>20</b>
<b>2.5 Definition of IS Resilience</b>	<b>21</b>
<b>2.5.1 Resilience and Situation Awareness</b>	<b>22</b>
<b>2.5.2 Resilience and Risk Intelligence</b>	<b>24</b>
<b>2.5.3 Resilience and Management of Vulnerabilities</b>	<b>24</b>
<b>2.5.4 Resilience and Adaptive Capacity</b>	<b>25</b>
<b>2.5.5 Resilience and Flexibility</b>	<b>25</b>
<b>2.5.6 Resilience and Agility</b>	<b>26</b>
<b>2.6 Distinguishing IS Resilience with Disaster Recovery planning and Business Continuity Management</b>	<b>26</b>

<b>2.7</b>	<b>Planning and Resilience</b>	<b>29</b>
<b>2.8</b>	<b>IS Resilience and Planning</b>	<b>31</b>
<b>2.9</b>	<b>Agency Theory Effects in Organisations</b>	<b>34</b>
<b>2.10</b>	<b>Agency Theory Effects in Decision Making</b>	<b>40</b>
<b>2.11</b>	<b>Weill's IT Governance Framework and Decision Making</b>	<b>41</b>
<b>2.12</b>	<b>COBIT and ITIL</b>	<b>46</b>
<b>2.13</b>	<b>Leadership</b>	<b>48</b>
<b>2.14</b>	<b>Culture</b>	<b>49</b>
<b>2.15</b>	<b>Crisis Management and Top Management Responsibilities</b>	<b>50</b>
<b>2.16</b>	<b>Decision-Making Under Uncertain Situation</b>	<b>53</b>
<b>2.17</b>	<b>Risk Preferences and Prospect Theory</b>	<b>56</b>
<b>3.</b>	<b><i>Conceptual Research Model</i></b>	<b>60</b>
<b>4.</b>	<b><i>Research Method</i></b>	<b>61</b>
<b>4.1</b>	<b>Q-Methodology and Q-Sort</b>	<b>61</b>
<b>4.2</b>	<b>Reliability and Validity in Q-methodology</b>	<b>63</b>
<b>4.3</b>	<b>Instrument Development</b>	<b>64</b>
<b>4.4</b>	<b>The Q- Sample</b>	<b>65</b>
<b>4.5</b>	<b>Description of Second Instrument</b>	<b>70</b>
<b>4.6</b>	<b>Pilot Test</b>	<b>71</b>
<b>4.7</b>	<b>A Brief Introduction to Jade Software Corporation</b>	<b>72</b>

<b>5.    <i>Research Findings and Discussion</i></b>	<b>74</b>
<b>5.1    Theoretical Framework</b>	<b>82</b>
<b>5.2    Strategy-Implementation Bi-cycle</b>	<b>87</b>
<b>5.3    How do senior executives make decisions</b>	<b>90</b>
<b>5.4    Necessary Elements of an IS Resilience Framework</b>	<b>94</b>
<b>6.    <i>Conclusion, Contribution and Future Research</i></b>	<b>96</b>
<b>8.    <i>References</i></b>	<b>101</b>
<b>9.    <i>Appendix A</i></b>	<b>109</b>

## ABSTRACT

*Organisational resilience has gained increasing attention in recent years. In this research, we adopt Agency Theory and Weill's IT Governance framework to investigate the decision priorities of senior executives in the context of IS resilience planning. IS resilience planning falls under the broader umbrella of IT governance and on an aspect of organisational resilience, that is, on Information Systems (IS) resilience. To the best of our knowledge, there is no study focusing on understanding the decision-making process of senior executives in relation to IS resilience. Although research has been undertaken on the topics of organisational resilience, and IT governance, there is a gap in the literature with respect to IS resilience. This research employ Agency theory combined with Weill's IT Governance framework to develop a conceptual framework, focused on decision-making and planning for IS resilience.*

*Concourse theory and Q-methodology were used to develop a Q-sort questionnaire, which was refined through interviews with researchers, decision makers from large and small organisations and IS professionals. For the purpose of this research 37 statements were sorted by key decision makers of the Jade Software Corporation, a large private organisation in New Zealand. We report a case study of the Jade, in which we have used Q-methodology to develop a typology of decision priorities for IS resilience planning. The Q-methodology is preferred in research where subjective opinion is to be explored with the goal of developing a typology, since it correlates the individual viewpoints of people rather than correlating variables selected in advance by the researchers. After the senior executives at Jade sorted the Q-statements, in-depth qualitative interviews were conducted to better understand their decision priorities. Detailed analysis revealed two types of decision makers in top management team, each representing a unique perspective of IS resilience. These types are discussed, along with*

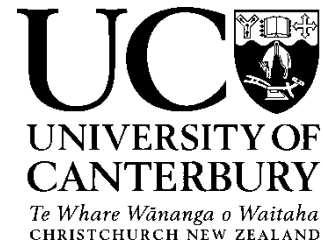
*implications of findings, a theoretical framework for IS resilience, and suggestions for future research.*

*This research also presents an in-depth case study of Jade adapting in the aftermath of a crisis, lessons learnt from them and also proposes a model for IS resilience planning based on IT governance framework. Moreover, this study shows how Q-Methodology can deepen our understanding of top management decision priorities in context to IS resilience planning, especially in crisis situation, addressing the general question: “How do senior executives in organisations make decisions under crisis situation and how do they prioritise their decisions to ensure IS resilience within their organisation?” It also asks the specific question: “How do senior executives at Jade Software Corporation make decisions under crisis situation and how do they prioritise their decisions to ensure IS resilience at Jade Software Corporation?” Given the potentially devastating implications of disruptions to organisations, understanding the dynamics of the successful adaption of IS within organisations indicates an important avenue for future research. This study provides a valuable contribution to our understanding of Information Systems resilience in organisations.*

*Keywords: Agency Theory, IT governance, IS resilience, TMT decision priorities, strategic decision making, decision rights, Top Management Team, IS Decision making, Crisis, Uncertain situation.*







Deputy Vice-Chancellor's Office  
Postgraduate Office

### Co-Authorship Form

This form is to accompany the submission of any thesis that contains research reported in co-authored work that has been published, accepted for publication, or submitted for publication. A copy of this form should be included for each co-authored work that is included in the thesis. Completed forms should be included at the front (after the thesis abstract) of each copy of the thesis submitted for examination and library deposit.

Please indicate the chapter/section/pages of this thesis that are extracted from co-authored work and provide details of the publication or submission from the extract comes:

*Section heading : Brief Introduction to Jade Software Corporation and First part of Research Findings and Discussions*

- Sarkar, A., Wingreen, S.C. and Ascroft, J. (2016) *Top management team decision priorities to drive IS resilience: lessons from Jade Software Corporation*. San Diego, CA, USA: 22nd Americas Conference on Information Systems (AMCIS 2016), 11-14 Aug 2016.(in press). (Conference Contribution - Other - Full conference papers).

Please detail the nature and extent (%) of contribution by the candidate:

*100% contribution by the candidate. Co-authors advised and validated the work produced by the candidate.*

### Certification by Co-authors:

If there is more than one co-author then a single co-author can sign on behalf of all

The undersigned certifies that:

- The above statement correctly reflects the nature and extent of the MCom (Hons) candidate's contribution to this co-authored work
- In cases where the candidate was the lead author of the co-authored work he or she wrote the text.

Name: *Stephen Wingreen* Signature:

A handwritten signature in red ink, appearing to read 'Stephen Wingreen'.

Date: *18 July 2016*

Deputy Vice-Chancellor's Office  
Postgraduate Office

### Co-Authorship Form

This form is to accompany the submission of any thesis that contains research reported in co-authored work that has been published, accepted for publication, or submitted for publication. A copy of this form should be included for each co-authored work that is included in the thesis. Completed forms should be included at the front (after the thesis abstract) of each copy of the thesis submitted for examination and library deposit.

Please indicate the chapter/section/pages of this thesis that are extracted from co-authored work and provide details of the publication or submission from the extract comes:

*Section heading Research Findings and Discussions. Specifically, last part of Research Findings and Discussions: Strategy-Implementation Bi-Cycle Model and How do senior executives make decisions.*

- Sarkar, A., Wingreen, S.C. and Ascroft, J. (2016) *Governing information systems resilience: a case study*. Krakow, Poland: European, Mediterranean & Middle Eastern Conference on Information Systems 2016 (EMCIS2016), 23-24 Jun 2016. (Conference Contribution - Other – Full Conference Paper)
- EMCIS 2016 Best Paper Award. Governing information systems resilience: a case study.

Please detail the nature and extent (%) of contribution by the candidate:

*100% contribution by the candidate. Co-authors advised and validated the work produced by the candidate.*

### Certification by Co-authors:

If there is more than one co-author then a single co-author can sign on behalf of all

The undersigned certifies that:

- The above statement correctly reflects the nature and extent of the MCom (Hons) candidate's contribution to this co-authored work
- In cases where the candidate was the lead author of the co-authored work he or she wrote the text

Name: *Stephen Wingreen* Signature: 

Date: *18 July 2016*



## 1. INTRODUCTION

Organisations increasingly rely on complex Information Systems (IS) and digital platforms to manage their businesses, which require IS to operate reliably under a variety of adverse circumstances. When interruptions affect IS operations, entire organisational ecosystems suffer from the disruption (Maurer & Lechner, 2014). One crucial aspect of examining organisational resilience is to examine the continuance of stable and reliable IS services (Gibb & Buchanan 2006). Previous research has addressed disaster recovery, continuity planning, crisis planning, and other relevant issues. Organisational research has included all of these issues in the concept of ‘organisational resilience’, which is generally defined as the organization's ability to operate reliably in a variety of adverse circumstances, but the concept of IS resilience has yet to be developed. In theory, IS resilience should be aligned with the overall organisational strategy, and therefore be placed under the wider umbrella of organisational resilience.

To date, there has been no systematic examination of how IS resilience planning decisions are made. Rather than inspecting previous failures and reveal finer details of what really happened and how to prevent a recurrence (Kayes, 2015), most research focuses on the IS planning agenda, and developing best practice for IS planning and priorities. For example, prior literature has discussed why IS planning should be undertaken, how IS plans can mitigate risks and how IS plans can be better connected to business strategy. We see three problems with this prior research in particular. First, it is mainly prescriptive in nature. Secondly, it describes what organisations should be doing with respect to IS planning practices, rather than what decision makers in organisations are actually doing and why they are doing so. Thirdly, IT governance is on the agenda of many organisations but having a high level IT governance

model does not ensure that governance is essentially working in the organisation. So, more research is needed to extend IT governance concepts to IS resilience. To our knowledge there are no empirical studies which address these three limitations, therefore this will be an important contribution of this research. This research gap is surprising, as resilience is often said to be a combination of organisational and technical qualities and, therefore, a research topic well suited for IS research (Muller, Koslowski & Accorsi, 2013).

Agency Theory has demonstrated significant predictive power with respect to the decision-making of owners and managers by its proposition of the principal-agent relationship dynamics (Eisenhardt, 1989; Jensen & Meckling, 1992; Lee & Wingreen, 2010). Specifically, Agency Theory proposes that the misalignment of interests between the principals (owners) of a firm and the agents (managers) is a source of costs and losses to the firm (Eisenhardt, 1989; Jensen & Meckling, 1992). When there are conflicting interests between principals and agents, it is referred to as "principal-agent conflict", which is solved by various types of contractual agreements that distribute risk among decision makers. However, Agency Theory does not deal directly with IT-related decision-making or risk distribution.

On the other hand, Peter Weill's IT governance framework (Weill & Ross, 2004) explains how decision rights and responsibilities are distributed within the IS function in organisations, by his definitions of IT archetypes, and IT domains, but it does not explain why decision rights and responsibilities are distributed the way they are. Agency Theory and Weill's framework are compatible with regard to both decision rights and decision responsibilities, since Weill's definition of an IT archetype encompasses the type of person who has decision rights, and the IT domain includes the decision responsibilities of each IT

functional area. Weill explicitly assumes that there should be alignment of decision makers' interests with the strategic interests of the firm, as it is with Agency Theory.

According to Weill and Ross (2004), IS resilience is comprised of a complex structure and process of decision-making which include alignment between IT and business strategies, improved focus on IT investment for strategic priorities, avoiding potential business risks, and capitalising on current business opportunities. For example, an IBM study reported how organisations are increasingly adopting integrated business resilience strategies in an uncertain environment and large organisations lead the way in business and IS resilience (IBM, 2011). So, IS resilience encompasses a variety of IT decision types, while some decisions have a clear strategic orientation, others may address strategic and business related objectives and the rest may lie somewhere in between. Also, an IS resilience plan is unique with respect to other types of plans because an IS resilience plan is intended to be implemented and executed during a time of a crisis situation, when there is a high degree of uncertainty and ambiguity. As previously noted in theory, IS resilience should be aligned with the overall organisational strategy, and therefore fall under the wider umbrella of organisational resilience.

Increasingly, IT governance receives a lot of attention with both academic and practitioners as the advantages of IT governance are being recognised (Grover, Henry & Thatcher, 2007; Weill and Ross, 2004). It is therefore the goal of this research to develop and validate an IT governance framework in the context of IS resilience. Toward this goal, we have selected Jade Software Corporation because it is an exemplar of the theoretical concepts we would expect in the context of IS resilience. Specifically, first of all, there is a strict separation of ownership and control between Jade's board of directors and their executive management team, as the key decision makers do not bear a major share of the wealth effects of their decisions. Secondly,

during the course of this investigation, Jade was actively involved in the domain of IS resilience planning, prioritization, and alignment in the aftermath of a major crisis: the Christchurch earthquakes of 2011. In this environment, we expect to observe all the richness of IS resilience decision priorities that our theory might predict. Therefore, this study aims to examine:

**RQ : How do senior executives make and prioritise decisions to ensure IS resilience?**

This study presents the findings of an investigation of the IS resilience decision priorities and decision-making process of the executive management team at Jade Software Corporation. First, the study reviews the literature on organisational resilience, IT governance, IS planning and agency theory is reviewed. Secondly, the study describes the research methodology, in which the Q-methodology is employed to determine how senior executives at Jade manifest their decision priorities and preferences in order to ensure IS resilience. Further, the study describes and analyses the interviews with the executive management team to enrich the interpretation of the case study. The research concludes with the discussion of a theoretically-founded typology of IS resilience planning priorities and concludes with the discussion of necessary components of IS resilience planning framework. In conclusion, the study discusses the relevance of this research for both practitioners and academics and proposes some recommendations for further research in the area of IS resilience.

## **2. LITERATURE REVIEW**

### **2.1 Hazards and Threats**

Natural disasters, pandemic disease, and terrorist attacks all pose a severe threat to the continuity of an organisation's operation. Disasters can cause challenges to organisations and it is essential to direct adequate effort into making them robust and resilient to withstand various uncertainties and challenges. While continuous and uncompromising effort to limit the human cost of disastrous events is necessary, the continuance of organisational activities and speedy recovery from damages should also be considered priorities. To a large extent, most organisations are dependent on information systems (IS) in their activities. As observed by Gibb and Buchanan (2006) in an event of a major disruption to the IS services, it is practically impossible for the businesses to function with snail mails and paper based accounting. Therefore, when examining the crisis resilience of organisations, one crucial aspect is to examine the continuance of stable and reliable IS services. Vijayraman and Ramakrishna (1993) characterise threats into three categories:

#### **2.1.1 Natural threats**

First type of threats come from natural disasters. Examples of natural disasters include fire, flood, earthquake, hurricane, tornado, snow storm, etc. Natural disasters pose external threats for IS assets such as data, hardware, software, personnel, and facilities (Vijayraman & Ramakrishna, 1993).

#### **2.1.2 Technical threats**

Second type of threats originate from technical failures of software applications when implemented. Technical failures are associated with unreliable equipment and



applications, power outages, and the system's failure to satisfactorily meet users' requirements (Vijayraman & Ramakrishna, 1993).

### **2.1.3 Human threats**

Third type of threats are man-made disasters. They can be further sub-divided as accidental or deliberate (Vijayraman & Ramakrishna, 1993). Accidental disasters can be caused by carelessly misplacing, erasing, or modifying data, software, and documentation. Deliberate man-made disasters result from theft, sabotage, and tampering of hardware, software, data, and documentation (Vijayraman & Ramakrishna, 1993).

## **2.2 Hazards in New Zealand Organisations**

According to Vargo & Seville (2011) many organisations look at the above list of major threats and would say either 'this is too unlikely' or 'I am too small and don't have the resources to influence the outcome'. In reality, New Zealand organisations are exposed to a wide range of natural hazards, both geological and weather related (Hatton, Seville, & Vargo, 2012). On 4 September 2010, a magnitude 7.1 earthquake occurred 40km west of the Christchurch Central Business District (CBD) at 4.35 a.m. This event caused substantial damage to property; however there was no loss of life. At that time, rebuild and repair costs from the earthquake were estimated at \$5 billion (Hatton, Seville, & Vargo, 2012). Regrettably, this event was the antecedent of the more devastating magnitude 6.3 earthquake, 13km south east of the central business district at 12:51 p.m. on 22 February 2011 which caused 185 deaths and widespread damage to the central business district as well as many residential areas. The combined losses of these two major earthquakes were estimated at over NZD 30 billion (Hatton, Seville, & Vargo, 2012).

Organisations with limited financial and human resources to respond are highly vulnerable in times of crisis. Organisations need to invest in their ability to respond quickly to changing environments; too few though fully develop this capability to improve their resilience to major crises (Ingirige and Wedawatta, 2011). A recent survey by Penn, Schohen & Berland, (2011) has identify that, when it comes to planning for a crisis, there are three types of companies. They can be categorised as:

- (a) Boy Scout (Well Prepared) - Companies with strong, comprehensive plans, which will stand up to the pressure of a crisis.
- (b) Tightrope walker (Vulnerable) - Companies with plans that will not necessarily cover them, or which aren't sufficiently comprehensive.
- (c) Ostrich (Exposed) – Companies who lack plans entirely, they see only barriers to creating plans and thus avoid making them.

According to (Crichton, 2006), businesses are likely to implement various generic coping strategies that aid business continuity, rather than organisational-level protection measures against crisis. Confirming this, Ingirige & Wedawatta (2011) reported that most organisations tend to rely on general business continuity or risk management strategies, although the uptake of those strategies was also found to be minimal. Vargo and Seville (2011) identify that the natural agility of many organisations contributes to their resilience but their lack of focus on planning can weaken their ability to find the 'silver lining'. In this context it is relevant to mention that, IBM (2011) reported that large organisations will lead the way in organisational resilience.

### 2.3 Resilience of Organisations

Gibson and Tarrant (2010) present the integrated functions model which proposes that organisational resilience is a goal that results from a combination of activities such as risk management and business continuity.

Not satisfied with the rigor of the integrated function model, Gibson and Tarrant (2010) later derive the herringbone resilience model shown as Figure 1. This model recommends that resilience is improved by a blend of an organisation's characteristics and their activities and capabilities (Gibson & Tarrant 2010). The herringbone model includes many of the factors considered as possible indicators of IS resilience.

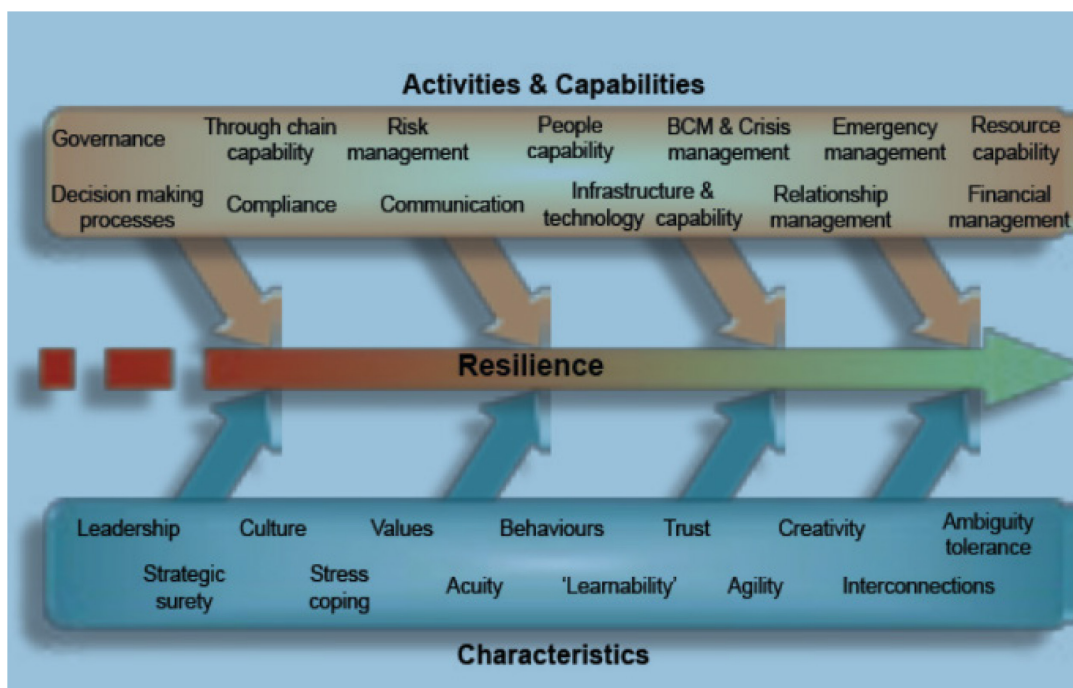


Figure 1. Herringbone Resilience Model (Gibson & Tarrant 2010)

The 'herringbone model' recognises that an organisation holds a substantial range of capabilities and undertakes a range of activities that will contribute towards improved resilience. Furthermore, the organisation also exhibits a number of characteristics that will

affect the effectiveness of the capabilities and activities and help to enhance the organisation's resilience (Gibson & Tarrant 2010).

## **2.4 Importance of IS Resilience in Organisations**

According to Gurbaxani and Whang (1991), the adoption of information technology (IT) in organisations has been growing at a fast pace. They suggest that the use of the technology has progressed from the automation of structured processes to systems that are truly radical as they introduce change into fundamental business procedures.

For most organisations today, much business is done with suppliers and customers on the Internet. Organisations rely heavily on IS and data, and operate 24/7. For this reason, the line between business and Information Systems (IS) is unclear (Sayana 2005). In present time businesses do not have any other means of recording transactions and data, as a result cannot afford to be without IS for long. In such situations, continued availability of IS is a prerequisite for business. In other words, all businesses that use IS and data in their operations have a need for business continuity and a disaster recovery plan. Most large organisations, particularly all Fortune 1000 enterprises, conduct regular IS audits to ensure confidentiality, integrity and continuous availability of IS (Singleton 2011). Hence, continued availability of information systems is one of the major criteria for IS resilience. Tsai and Sang (2010) argue that in present era information continuity equals business continuity. Information Systems (IS) are considered as the most vulnerable components in delivering continuous services (Maurer & Lechner, 2014).

## 2.5 Definition of IS Resilience

The concept of resilience has been a noticeable and emerging topic in various scientific fields, such as ecology, psychology and engineering. However, as resilience encompasses a wide range of different research contexts and topics, it is not surprising that the concept lacks an accepted common definition across disciplines (Muller, Koslowski and Accorsi, 2013). Rooted from the word *resilire*, meaning to spring back or to rebound, the term refers to ‘the ability to recover form and position elastically’ (Muller, Koslowski & Accorsi, 2013). Against this background, resilience is defined as “the ability of an organisation to not only survive but to thrive, both in good times and in the face of adversity” (Seville 2009). Vargo and Stephenson (2010) proposed that for organisations to invest in resilience, the business case for resilience investments has to go beyond insurance, and must be as good as the business cases for new equipment or new staff.

We observe that some notions which are frequently identified as attributes of resilient systems are flexibility, agility, adaptive capacity and robustness. Weick, Sutcliffe and Obstfeld (2008) defined a narrower definition of resilience, “the capacity to balance and sustain desired state under difficult and challenging event”, which only deals with the recovery aspect of resilience. Madni and Jackson (2009) differentiates between two types of resilience : reactive and adaptive. While reactive resilience implies immediate or short term remedial action, adaptive resilience refers to long-term proactive measure and is closely bolted by situational awareness and understanding and managing key vulnerabilities. In this research we will focus on the adaptive resilience of the organisations. Madni and Jackson (2009) also identify that resilience is highly related to safety, reliability and survivability. Where safety is defined as the ability of a system to understand how it can proactively ensure things to stay under control; reliability is defined as the ability of a system to perform required functions under crisis

conditions and finally, survivability is the ability to withstand attacks or the ability to minimize the impact.

### **2.5.1 Resilience and Situation Awareness**

While there are many definitions of situation awareness, the one best suited to the context of this research is “a continuous extraction of environmental information, integration of this information with previous knowledge to form a coherent mental picture, and the use of that picture in directing further perception and anticipating the future” (Vargo & Seville, 2011).

Vargo and Seville (2011) mention that any effective planning process involves an organisation to be alert to and monitoring the organisational environment so that it can more effectively align its capabilities and resources with threats and opportunities. They also argue that a major insufficiency of conventional strategic planning is the lack of sensitivity and inability to deal with the discontinuities and crises that arise in a dynamic and turbulent environment. To address the issue related to lack of sensitivity, a parallel discipline of strategic issues management has evolved, but there are concerns that this lacks some of the visioning, enduring and motivational qualities of traditional strategic planning (Vargo & Seville, 2011).

“Managers worldwide have begun to focus less on the task of forecasting and planning for the future and more on the challenge of being highly sensitive to emerging changes” (Vargo & Seville, 2011). In other words, this requires organisations to develop strategies for actively improving their level of situation awareness. Vargo and Seville (2011) also observe that in dynamic situations, the things that are important and the things that are irrelevant can change with little notice. In these situations, recognising patterns emerging from the ‘un-order’ can be more productive than collecting and analysing data in order to make rational decisions (Vargo & Seville, 2011).

In the same line of thought, Mitroff (1988) emphasises the importance of being alert to the early warning signals that occur long before a crisis occurs. He theorises that proactive organisations are more resilient organisations and are always looking for early warning signals and are more expected to have verified response and recovery plans in place. On the other hand the reactive organisations tend to ignore these signals and even block them intentionally.

While there are challenges for organisations to effectively build situation awareness to inform their medium and longer term strategic planning, these challenges are augmented in fast evolving crisis environments. Vargo and Seville (2011) prescribe that not only do individuals responding to crises need to build their situation awareness, the crisis management team need to build a shared awareness of the situation they are facing. Also, team situation awareness requires the additional elements of coordination and information sharing (Vargo & Seville, 2011). According to Vargo and Seville (2011), ways to prepare decision makers for this task may include: (1) building a clear sense within the team of the overall mission of the group and how the different team members contribute to this mission, (2) defining clear roles so that team members are monitoring different segments of the environment, with sufficient overlap to promote collaboration, and (3) developing processes for exchanging and validating information between individual team members so there are sufficient opportunities to compare and update 'individual mental models' of the situation. It is worth mentioning that the safety attribute of resilience as identified by Madni and Jacson (2009) is comparable to the concept of situation awareness

### **2.5.2 Resilience and Risk Intelligence**

Disruptive events are defined as random events caused by internal and external factors affecting a system that have a negative impact on system operations. The performance of the system fluctuates in proportion to the impact of the disruption. The resilience of the system depends on how much change there is to the performance of the system during a disruptive event and the time lapse from the first impact of the disruptive event to full recovery. There are two distinctive perspectives in the resilience literature regarding preparation for the disruptive events. First perspective states, resilience relies upon the anticipating unexpected disruptive events and designing solutions to eliminate errors (Hollnagel et al. 2006). The other perspective suggests that resilience relies more on detecting unexpected events sooner, when they can be more easily corrected, in addition to building the capacity to recover from such events (Weick & Sutcliffe 2007). Risk intelligence is defined as the ability to identify and anticipate risks.

### **2.5.3 Resilience and Management of Vulnerabilities**

“Resilience of a system is measured by the level of its vulnerability to a specific risk” and vulnerability is defined as being at risk and the probability of having disruptions” (Sheffi & Rice 2005). They suggest that reducing vulnerability has a positive impact on the resilience of a system (Sheffi & Rice 2005). Sheffi and Rice (2005) strongly recommend that vulnerability assessment should be a part of strategic planning for resilience. They define the level of vulnerability as the probability of the occurrence of a disruption and the extent of the subsequent consequences. As the probability of the occurrence of any disruption and the severity of the consequences increases, the system’s vulnerability quotient will be higher. The



reliability attribute of resilience as identified by Madni and Jacson (2009) is very similar to the concept of management of vulnerabilities.

#### **2.5.4 Resilience and Adaptive Capacity**

Adaptive capacity is a concept that has also been commonly associated with resilience (Dalziell & McManus 2004). Dalziell and McManus (2004) advise that in order to enhance resilience, adaptive capacity should be increased even after a disruption. Dalziell and McManus (2004) define adaptive capacity as an aspect of resilience that echoes learning; the flexibility to experiment and adopt novel solutions and development of generalised responses to broad classes of challenges. Adaptive capacity has also been related to concepts of robustness, agility and adaptability. Adaptive capacity point out the ability of systems to return to their initial state after partial damage, while robustness entails that systems do not get any damage at all (Dalziell & McManus 2004). Adaptability demonstrates the ability to adapt to changing environments while delivering the intended functionality under varying operating conditions. It is worth noting that the survivability attribute of resilience as identified by Madni and Jacson (2009) is very similar to the concept of adaptive capacity.

#### **2.5.5 Resilience and Flexibility**

Flexibility has become an emerging construct of resilience in the literature (Sheffi & Rice 2005). Studies related to resilience recommend that the adaptive capacity of a system in the case of a disruption can be increased by designing, planning and building flexibility in systems (Sheffi & Rice 2005). Flexibility may be defined as the ability of a system to adapt to the changing requirements of its environment and its stakeholders with minimum time and effort. Dalziell and McManus (2004) relate flexibility to agility and adaptability suggesting that flexibility is a system's ability to rapidly adapt to its changing environment. Muller et al.

(2013) link the concept of resilience with flexibility by stating that resilience is a system's ability to bounce back from disruptions and disasters by building in redundancy and flexibility.

#### **2.5.6 Resilience and Agility**

Agility has been commonly used in combination with flexibility as a defining attribute of resilience. Agility characterises a system's ability to change rapidly (Fricke & Schulz 2005). Helaakoski (2007) defines agility as the system's ability to respond to changes in an uncertain and quickly evolving environment. According to Christopher and Peck (2004), resilience involves agility and it helps a system to rapidly rearrange itself. Dalziel and McManus (2004) relate agility to high resilience organisation characteristics. Morello (2001), on the other hand, suggests that agility may introduce new risks and vulnerabilities which may result in lower resilience.

### **2.6 Distinguishing IS Resilience with Disaster Recovery planning and Business Continuity Management**

Much research has been done in Disaster Recovery Planning (DRP) and Business Continuity Management (BCM) topics. So, it is important to distinguish IS resilience from Disaster Recovery Planning (DRP) and Business Continuity Management (BCM). According to Maurer and Lechner (2014), while DRP takes care of the continuity of IS services and it is mostly technical in nature and typically focuses on restoring critical business processes and related to Information Systems. BCM does not only address the information systems outage as the only threat but also addresses other non - technical organisational threats and vulnerabilities. Thus, BCM has its roots in DRP and includes IS. Citing Madni and Jackson (2009), Maurer and Lechner (2014) argue that resilience is a multi-faceted capability that includes avoiding, adapting to, absorbing, recovering and thriving from crisis. According to

Madni and Jackson (2009) a resilient framework may be achieved when the organisation is able to bounce back. In order to bounce back Madni and Jackson (2009) suggest that, organisation should be able to avoid, survive and recover from sudden disruptions. The organisation should be resilient enough to provide continuous critical services and must ensure the continued existence of critical data and systems. They must also have a robust and agile communication system in place and should be able to identify and rectify the root cause as quickly as possible.

Moreover, Maurer and Lechner (2014) identify DRP as a critical component of IS resilience and BCM as a prerequisite to strengthen the IS resilience as well the organisational resilience. So, on one hand, DRP and BCM are seen as frameworks to develop IS resilience and on the other hand, IS resilience supports and enhances DRP and BCM. IS resilience extends the recovery views and adds overall situation awareness, decreased vulnerabilities and increased adaptability, risk intelligence, flexibility and agility attributes as identified by McManus et al. (2008).

After an extensive literature review we have not been able to find a definition of IS resilience. However, organisational resilience has been studied extensively by researchers (Vargo & Seville, 2011; Hatton, Seville, & Vargo, 2012).

A definition of Information Systems resilience is introduced based on these characteristics for the purpose of our study, it is defined as:

*Information Systems resilience is a function of an organization's overall situation awareness related to Information Systems, management of Information Systems vulnerabilities, and*

*adaptive capacity, risk intelligence, flexibility and agility of Information Systems in a complex, dynamic, and interconnected environment.*

In order to define IS resilience we have utilised six attributes as identified by McManus et al (2008), namely overall situation awareness, decreased vulnerabilities and increased adaptability, risk intelligence, flexibility and agility. These terms are defined in Table 1.

<b>Set of Attributes</b>	<b>Definition</b>
Situation awareness	It is the ability to identify and understand changes in the environment.
Management of Vulnerabilities	It is the capability to deal with the major vulnerabilities.
Adaptive Capacity	It is the capability to respond to and adapt to the changing environment.
Risk Intelligence	It is the ability to identify and anticipate risks.
Flexible	It is the ability to change.
Agile	It is the ability to produce timely responses to changing environment and conditions.

*Table 1. Attributes of IS resilience*

The traditional approach is to define resilience focuses on an event based, reactive approach that deals with identifying potential risks and preparing response measures for each of them. Whereas, our definition of IS resilience incorporates a process based, proactive approach to build sustainable resilience model. The process based approach embeds the resilience thinking, preparedness and planning in to the culture of an organisation, which distinguishes it from merely prescribing a corrective measure for a particular event (Vargo and Seville, 2011). It is worth mentioning that due to growing dependency on information systems it is hard to distinguish information systems

continuity from business continuity. In other words, for many businesses information systems continuity and business continuity are the same.

## **2.7 Planning and Resilience**

Discussion on resilience is incomplete unless we explore planning. Zheng et al (2013) state that continuity planning is a vital requirement. They stress that organisations who experience a disruption and do not have *Disaster Recovery Plan* (DRP) and *Business Continuity Plan* (BCP) in use will ultimately fail. A central theme of resilience research is the questions of anticipation vs. resilience, and planning vs. adaptation. Anticipation includes predicting possible sources of crisis or disaster. So that sources of crisis can be planned for, mitigated, or even avoided. Weick and Sutcliffe (2007) refer to this as avoiding error by design, whereby a system of controls, processes and barriers is put in place to avoid possible crises from happening. Weick and Sutcliffe (2007) further add that an anticipatory approach is more suited to environments characterised by stability and predictable outcomes.

The primary objective of detailed, formalised planning is to reduce uncertainties (Simon, 1997). One such example of detailed planning process is creation of DR and BC plans. These plans are documents that provide detailed guidelines, contact information and procedures for how information should be shared during all phases of an unexpected occurrence that requires immediate action.

A strong DR and BC plan provides step-by-step instructions for how to deal with a crisis. These plans identify important people and their backups, explains how information should be communicated and documents what procedures will be enacted to track and share company and individual employee status (Grant, 2003). In the event of an emergency, these plans must be able to launch quickly, brief senior management as soon as possible,

communicate information to all interested stakeholders and anticipate the need for changing communication channels as events develop (Grant, 2003).

These plans may also address ways both electronic and non-electronic communication channels can be used to disseminate information. This includes announcements over a building paging system, automated text message or email alerts. When electronic communication channels be available, social media and the organization's website can also be used to communicate emergency information. Although automated emergency notification systems can enhance these plans, a traditional landline call tree should also be part of the plan in case Internet or cellular service is disrupted (Grant, 2003).

This formalised approach to planning has come under attack from scholars (Grant, 2003; Premkumar & King, 1994; Hamel, 1996). According to Hamel (1996), ‘ in the vast majority of companies, planning is a calendar-driven ritual .....[which assumes] that the future will be more or less like present’.

In contrast, resilience involves being flexible in a changing environment. Weick and Sutcliffe (2007) discuss the resilience approach and note that resilient organisations recognise that it is impossible to prevent all crises and disasters all of the time. Instead they monitor their organisation as a system with inputs and outputs, the characteristics of which can provide information about the health of the whole system. Both planning and resilience involve the evaluation and prioritization of a multitude of factors, the prioritization of those factors with reference to one another, and decisions that ultimately reflect the priorities of the decision maker. Therefore it is necessary to adopt a strategy and methods that support prioritization of a multitude of decision criteria. Dey (2011) summarises that DRP and BCP experience low commitment and many organisations have little or any experience in planning, testing or

implementing them. Dey (2011) claims that while some organisations realise that without having an active BCP and DRP can put them in a vulnerable situation and others still try to protect themselves with business interruption services such as business continuity insurances.

Optimally, businesses should find the most effective balance, or “equilibrium” between anticipation and resilience. Comfort (2001) argues that disaster management practices are moving towards a combination of anticipation and resilience strategies. “While we agree that resilience is the key to coping, it is necessary to organise for resilience” (Comfort, 2001). Research also suggests that the anticipatory approach, including planning, is used to enable organisations to be resilient. Planning and formalising response arrangements in advance means that the organisation is free, at the time of crisis, to be much more adaptive and resilient in its response (Teoh and Zadeh 2013). Thus, instead of planning for an uninterrupted and continuous operation, a resilient organisation is able to recognise disturbances and evade risk with an ability to adapt and reconfigure as quickly as suitable, either to bring the organisation to the optimal operational position, or to converge to a new optimal operating position (Teoh & Zadeh 2013).

## **2.8 IS Resilience and Planning**

Empirical studies of IS planning practices in organisations indicate that varied differences exist. Organisations differ in terms of how much IS planning they do, the IS planning methodologies they use, the employees involved in IS planning, the alignment between IT and business, the focus of IS plans, and the ways in which IS plans are implemented (Hann & Weber, 1996). IS planning has been used to accomplish three major objectives: (1) establishing a basis for monitoring and bonding IS managers so their actions are more likely to be consistent with the goals of their superiors; (2) resolving how the gains and losses from

unforeseen circumstances will be distributed among principals and agents; and (3) determining the level of decision rights to be delegated to the agents (Hann & Weber, 1996). However, IS resilience planning is unique with respect to other types of plans because an IS resilience plan is intended to be implemented during a time of crisis or adverse circumstances, when there is a high degree of uncertainty.

IS planning plays a crucial role in today's complex, connected, unpredictable and dynamic corporate world. IT is fused into all aspects of business operations and the need for strategic IS planning is of great importance in achieving success. It is defined as the process of strategic thinking that identifies the most required IS on which the organisation can implement and impose its long-term IS activities and policies. Earl (1993) states that IS planning is a mixture of formal activities and informal behaviour. It can either be a special effort or part of overall organisational planning. However, very few organisations successfully adapt to the demands of constant change by strategic use of IS.

Moreover, if decision rights are not delegated in the presence of high uncertainty, organisations cannot respond quickly enough to the IS prospects and problems they meet. IS resilience shares some commonality with crisis management. Crisis management is the process by which an organisation deals with any major unpredictable event threatening to harm the organisation, its stakeholders, and its customers and suppliers. Vargo and Seville (2011) point that three elements are common to most imageries of crisis: first, a threat to the organisation, secondly, the element of surprise, and thirdly, a short decision time frame. They argue that crisis planning is about building capability to identify impending threats to the organisation and designing a plan for addressing those threats. It is clear that IS resilience planning and crisis planning overlap considerably, they can be summarised as follows:



- they both deal with the future;
- they both deal with the weaknesses (vulnerabilities) and threats (risks)
- they both involve creating a plan
- they both involve organisational structures and resources to carry out the plan

However Vargo and Seville (2011) warn us that these two planning processes are typically carried out in isolation from one another, if they are carried out at all.

Prior studies of IS planning practices in organisations indicate that varied differences exist. Organisations differ in terms of how much IS planning they do, the IS planning methodologies they use, the employees involved in IS planning, the alignment between IT and business, the focus of IS plans, and the ways in which IS plans are implemented (Hann & Weber, 1996). IS planning has been used to accomplish three major objectives: (1) recognising organisational opportunities and problems where IS might be used successfully; (2) identifying resources required to allow IS to be applied successfully these problems and opportunities; and (3) developing strategies and processes to allow IS to be applied successfully to these opportunities and problems (Hann & Weber, 1996).

Thus, IS planning process is recognise as an exercise to improve organisations' strategic alignment with business-IT objectives; to meet short-term and long-term organisational needs; and to provide the ability of creating impact on competitive advantages. The goals of IS planning include improving systems' architecture; infrastructure capability and reliability from IS/IT investments; managing information resources effectively; and securing user satisfaction.

## 2.9 Agency Theory Effects in Organisations

Agency theory has its roots in economic theory and is based on the following principles.

“Agency theory is a contract under which one or more persons (the principals) engage another person (the agent) to perform some service on their behalf which includes delegating some decision-making authority to the agent. If both parties to the relationship are utility maximisers there is good reason to believe the agent will not always act in the best interests of the principal”.

(Jensen & Meckling, 1976)

According to Agency theory a firm is a production function for transforming inputs (e.g. labour, capital) into output (Jensen & Meckling, 1976). Agency theory discards the classical view of the firm as a unified profit-maximizing identity and proposes an alternative model of a firm as an agency relationship built on a set of contracts among self-interested agents (executives). As a result, when decision-making authority is delegated to agents, it cannot be guaranteed that the decisions will be aligned with the interest of the principal. The divergence of interests between the principals and agents can raise many problems and as a result is costly to a firm, commonly known as *agency costs*. Agency theory explains how a firm can be maintained as a viable form of economic organisation regardless of the presence of these problems (agency conflicts). Agency theory also predicts that the agency conflict may be reduced when the owner is involved in management (Fama & Jensen, 1983; Jensen & Meckling, 1976). In other words, with personal involvement in management, the principal could lessen the incentive for opportunistic behaviour and ensure the agent's decision will be aligned with the interest of the firm.

Fama and Jensen (1983) conduct their research on large firms where they studied how these firms survive when important decision agents do not bear a substantial share of the wealth effects of their decisions. They argued that separation of decision and risk-bearing functions can be observed in both large public and private organisations as well as in small firms. They stated that an organisation is inter-connection of contracts and these contracts specify the rights of each agent in the organisation and their performance criteria is evaluated on the basis of the contracts and also the payoff function they will face. In organisations the contract structures limit the risks undertaken by the agents by specifying either fixed payoffs or incentive payoffs attached to specific measures of performance. The residual claimants or residual risk bearers are the agents (executives) who are accountable for their own decisions.

Fama and Jensen (1983) mention in their research that the way organisations allocate the steps of the decision process across agents is significant in explaining the survival of organisations.

As described by Fama and Jensen (1983), the decision process has four steps:

- initiation—generation of proposals for resource utilization and structuring of contracts;
- ratification—choice of the decision initiatives to be implemented;
- implementation—execution of ratified decisions; and
- monitoring— measurement of the performance of decision agents and implementation of rewards.

Fama and Jensen (1983) also observe that as initiation and implementation of decisions are allocated to the same agents. So it is convenient to combine these two functions under the term decision management. Likewise, the term decision control may include the

ratification and monitoring of decisions. Decision management and decision control are the components of the organization's decision process or decision system Fama and Jensen (1983).

Fama and Jensen (1983) further state that, control of agency problems in the decision process is important when the decision managers who initiate and implement important decisions are not the major residual claimants and therefore do not bear a major share of the wealth effects of their decisions. According to Gurbaxani and Whang (1991) without effective control procedures, such decision managers are more likely to take actions that deviate from the interests of residual claimants (principals). An effective system for decision control implies, almost by definition, that the control (ratification and monitoring) of decisions is to some extent separate from the management (initiation and implementation) of decisions. Individual decision agents can be involved in the management of some decisions and the control of others, but separation means that an individual agent does not exercise exclusive management and control rights over the same decisions.

Gurbaxani and Whang (1991) observe that in a noncomplex organization, specific knowledge important for decision management and control is concentrated in one or a few agents. According to Agency theory when it is efficient to combine decision management and control functions in one or a few agents, it is efficient to control agency problems between residual claimants and decision makers by restricting residual claims to the decision makers. This proposition gets clear support from the proprietorships, small partnerships, and closed corporations observed in small-scale production and service activities. These organisations are all characterized by centralised decision systems and owners or principals that are restricted to decision agents (Gurbaxani & Whang, 1991).

Fama and Jensen (1983) state in their hypotheses about the relations between the risk bearing and decision processes of organisations.

1. Separation of residual risk bearing from decision management leads to decision systems that separate decision management from decision control.
2. Combination of decision management and decision control in a few agents leads to residual claims that are largely restricted to these agents.

They argue that control of agency problems in the decision process is important when the managers who initiate and implement important decisions are not the major residual claimants and therefore do not bear a major share of the wealth effects of their decisions. They further add that without an effective control mechanism such decision agents are more likely to take decisions that is different from the interests of the principals. They suggest that the control (ratification and monitoring) of decisions need to be separated from the management (initiation and implementation) of decisions.

According to Fama and Jensen (1983), the public organisations are tend to be noncomplex as oppose to the private organisations which tend to be complex. According to agency theory in a public organisation, specific knowledge important for decision management and control is concentrated in few agents. On the other hand in the complex private organisations it is common to see a formal decision hierarchy with higher level agents (board of directors) ratifying and monitoring the decision initiatives of lower agents (resilience committee) and evaluating their performance.

It is commonly observed in large organisations that the board of directors have the power to hire, fire and reward the top-level decision managers and to ratify and monitor

important decisions. Exercise of these top-level decision control rights by the board helps to ensure separation of decision management and control. In this context it is worth noting that decision functions in large organisations can be delegated in two general ways : first, joint delegation to several agents (as in a IS resilience committee), or secondly segregating and delegation of parts to different agents (as in giving sole responsibility of IS resilience to CIO or different aspect of IS resilience will have different decision maker). As the decision-making in large firms can be distributed among a team of decision makers so it is appropriate to include other key decision makers (for example other c-suite top managers) along with the CIO in this study.

Access to sources of funds and the amount of funding available are more in large organisations. This in turn may influence performance and ability to attract high quality managers. Large organisations (LO) may need to produce a performance objective formulated by the stakeholders. Performance objectives based on financial criteria are common in large organisations. Accordingly, given the importance of quarterly and annual results, large organisation managers are less likely to engage in risky projects (Eisenhardt, 1989). This in turn, is likely to influence the emphasis placed on the dimensions of strategy, the differential pursuit of short-term and long-term performance, leadership style, and motivation.

As large organisations operate under the conditions of a stronger cash flow and more equity reserves. Consequently, it is more likely that they have the capacity to compensate for occurring incidents or buffer themselves against Information System risks. Therefore, it is expected that large organisations will face less severe issues with the vulnerability of their IS. (Thun, Drüke, & Hoenig, 2011).

Zheng et al. (2003) explained in their research that large firms have huge purchasing power which may affect the purchasing behaviour of LOs. In their study, LOs with more purchasing power are keen to engage in the market, resulting in a continuous approach and further of strategic direction in their purchasing activities.

Carey (2008) suggests that the separation of ownership and management can cause agency conflict. The impact of ownership on organisational performance has attracted the interest of a large number of scholars (Fama & Jensen, 1983; Gurbaxani & Whang, 1991; Jensen & Meckling, 1976). Within larger and complex organisations an extended hierarchy of principals/agents can be found. Which may include the owner or shareholder through the board, top management and senior executives and middle management. It is important to understand that within each level in the hierarchy a personnel may have to act as principals to their immediate subordinates, all within the ultimate principle of agency theory (Gurbaxani & Whang, 1991). "Ownership represents a source of power that can be used to either support or oppose management depending on how it is concentrated and used" (Gurbaxani & Whang, 1991). It also impacts on the criteria used to select agents and the formality and thoroughness of the selection process. Public organisations are likely to deploy more elementary search and selection processes than the private organisations (Gurbaxani & Whang, 1991). Furthermore, the likelihood of interference by the principal is greater. These in turn may result in poor performance, weak and divided leadership, and a negative culture. Hence, we can conclude that public and private organisations also differed across a number of culture constructs. Based on the existing literature, we can expect to find large private organisations to have stronger culture.

Variyam and Kraybill (1993) speculate that ‘besides size, human capital, and market structure, a firm’s choice of strategies is likely to be affected by its ownership’. They suggest that strategic planning is more frequent in large organisations. On the other hand, scholars suggest that a considered strategy (that is to say, the outcome of the strategy making process), irrespective of size, enables organisations to develop and maintain sustainable competitive advantage (Roper, 1997). Such arguments suggest differences in performance due to ownership.

### **2.10 Agency Theory Effects in Decision Making**

Agency Theory rejects the classical view of the firm as a unified profit-maximizing identity and proposes an alternative model of a firm. Agency Theory is essentially a theory of decision-making, where the principal and the agent are theorised to be in a contractual agreement that serves the best interests of the principal (Eisenhardt, 1989; Jensen & Meckling, 1992). Conflict between the principal and the agent occurs when the agent pursues his or her own best interests rather than those of the principal, and the principal finds it difficult and costly to verify what the agent is actually doing; as a result, the firm becomes less efficient, and this situation is referred to as the “agency problem.” The central notion behind the Principal-Agent model is that the principal is too busy to do a given job and so hires the agent, but being too busy also implies that the principal cannot monitor the agent effortlessly.

When decision-making authority is delegated to agents, it cannot be guaranteed that the decisions will be aligned with the interest of the principal. However, when the principal has adequate information to verify agent behaviour, the agent is more likely to behave in favour of the principal (Eisenhardt, 1989). It predicts that higher levels of uncertainty will be associated with higher levels of delegation of decision rights to the agent. However, if decision



rights are not delegated in the presence of high uncertainty, organisations cannot respond quickly enough to the IS prospects and problems they meet. Generally speaking, Agency Theory also predicts that risk would be transferred away from lower levels of the firm, to be borne by senior executives and managers.

Although IS plans are usually about funding, functional activities (Hann & Weber, 1996), or IS processes, in the case of monitoring unobservable behaviours, the principal may use IS plans as a cost-effective means of monitoring and bonding agents (senior executives and managers) because they provide information about the agent's efforts to manage risk. Senior management may seek to exert more influence on the form of the IS plan via their control over the planning process if it can be used for monitoring and bonding purposes. From their viewpoint, the plan will be a better monitoring and bonding device if it reflects their goals and objectives rather than the IS manager's goals and objectives. In the context of Agency Theory, an IS plan is a form of implicit contract between the principals (Directors) and their agents (Sr. Executives), and between senior executives and employees at other levels of the firm. An IS plan is thus a vehicle to distribute risk across all levels of the firm.

### **2.11 Weill's IT Governance Framework and Decision Making**

Decision rights imply a decision-maker with knowledge needed to make those decisions, since a decision right specifies who in a firm has the authority to make what decisions. Decision rights must be moved to the department where the relevant knowledge resides ("delegation" solution), or the relevant knowledge must be moved to the locus of decision rights ("transmission" solution) (Jensen & Meckling 1992). Therefore, IT governance has become an important issue in organisations. While there are many definitions of IT governance exist but the following two definitions are widely used in IS research.

*“IT governance is the responsibility of the Board of Directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategy and objectives”* (IT governance Institute, 2001).

*“IT governance is the organisational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT”* (Van Grembergen, 2002).

These definitions emphasise on the same aspects: alignment of business and IT, and the primary responsibility of the board and senior executives. Van Grembergen’s definition also specifies that IT management must participate in the IT governance processes. It is important to note that there is a clear distinction between IT management and IT governance. IT management is engrossed on the effective management of IT operations and supply of IT resources, whereas, IT governance is much larger concept and focusses on performance and transformation of IT to meet present and future demands of the business and its customers.

IT governance describes a firm’s overall process for sharing IS decision rights and monitoring the performance of IT investments (Weill & Ross, 2004). IT need to be governed to ensure corporate governance and it is evident from the definitions that IT governance is an essential part of enterprise governance and has a strong relationship with IS resilience. This relationship can be further established by translating the IT governance questions into specific IS resilience questions (refer to table 2).

IT Governance	IS Resilience
How does top management get the CIO and IT organisation to return some business value to it?	How does board get the senior executives to ensure IS resilience?
How does top management make sure that the CIO and IT organisations do not steal the capital it supplies or invest it in bad projects?	How does board monitor that the senior executives will prioritise and invest in the projects which will ensure IS resilience?
How does top management control the CIO and IT organisation?	How does board control the senior executives' decision priorities to ensure IS resilience?

*Table 2. IT governance questions are adopted from "IT Governance and Its Mechanisms" (Haes & Van Grembergen, 2004)*

IT governance, the term defined as "specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT" (Weill & Ross 2004) constitutes the most universal and systematic approach helping to solve the problems connected with supporting business with IT in the organisational context. There is a distinction between IT governance and IT management. Weill is speaking primarily of IS when he develops his IT governance framework, it does not focus on the technological solutions to business problems rather it focuses on principles of technologies as it relates to corporate businesses. "IS" is a term used primarily by academics, while "IT" is the term used in practice to speak of IS. According to Weill, IT governance is not about specific decisions about IT but about who makes what decisions, who has input and how the decision makers are held accountable for the decisions, in this case, IT governance includes IS.

IT governance encompasses five major decision domains (Weill & Ross, 2004). First, IT principles comprise the high-level decisions about the strategic role of IT in the business. Second, IT architecture includes an integrated set of technical choices to guide the

organization in satisfying business needs. Third, IT infrastructure consists of the centrally coordinated, shared IT services that provide the foundation for the enterprise's IT capability and were typically created before precise usage needs were known. Fourth, Business application needs are the business requirements for purchased or internally developed IT applications. Fifth, prioritization and investment decisions determine how much and where to invest in IT. There are six archetypal approaches to IT decision making, ranging from highly centralised to highly decentralised. Most companies employ a variety of them, using different approaches for different decisions (Weill & Ross, 2004).

Moreover, Peter Weill's IT governance framework describes how decision rights and responsibilities are spread within the IT function in organisations, by his definitions of IT archetypes, and IT domains, but it does not elucidate why decision rights and responsibilities are distributed the way they are or how the decision makers make decisions. Weill's definition of an IT archetype involves the type of professional who has decision rights, and the IT domain comprises the decision responsibilities of each IT functional area (Weill & Ross, 2004). Decision rights indicate a decision-maker with knowledge needed to make those decisions, since a decision right specifies who in a firm has the authority to make what decisions. Decision rights essentially moved to the department where the relevant knowledge resides ("delegation" solution), or the relevant knowledge must be moved to the locus of decision rights ("transmission" solution) (Jensen & Meckling 1992). As mentioned before, Weill explicitly assumes that there should be alignment of decision makers' interests with the strategic interests of the firm. According to Weill, IT governance is not about explicit decisions about IT but about who makes what decisions, who has input and how the decision makers are held accountable for those decisions. IT governance encompasses five major decision domains.

First, IT principles comprise the high-level decisions about the strategic role of IT in the business. Secondly, IT architecture includes an integrated set of technical choices to guide the organization in satisfying business needs. Thirdly, IT infrastructure consists of the centrally coordinated, shared IT services that provide the foundation for the enterprise's IT capability and fourth, business application needs are the business necessities for purchased or internally developed IT applications. Finally, prioritization and investment decisions determine how much and where to invest in IT. Also, there are six archetypal approaches to IT decision making, ranging from highly centralise to highly decentralise. According to Weill most enterprises employ a variety of them, using different approaches for different decisions (Weill & Ross, 2004).

Currently, there is a plethora of IT management frameworks and standards, each catering to a narrow silo. A general lack of clarity still exists, when it comes to what constitutes an overarching IT governance framework focused specifically on the senior management's role. IT governance, the term defined as “specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT” (Weill & Ross 2004) constitutes the most universal and systematic approach helping to solve the problems connected with supporting business with IT in the organisational context. IT governance can be deployed using a mixture of various structures, processes and relational mechanisms. A mixture of various structures, processes and relational mechanisms are deployed in organisations. IT governance structures include organisational units and their roles and responsibilities for making IT decisions. This can be proposed as an outline of how the IT governance framework will be structurally organised in an organisation. Further, IT governance processes refers to the formalisation of strategic IT decision making, IT monitoring and IT performance management

procedures. Processes are important to ensure that daily practices are consistent with policies and provide a feedback to decisions. Finally, relational mechanisms are about active support and participation of senior executives, IT management and business management. Relational mechanism include education, training and empowerment of employees. An example of these structures, processes and relational mechanisms are provided in figure 2.

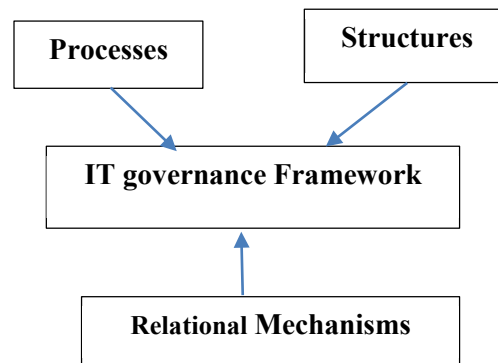


Figure 2. IT governance framework

In this research the focus is on who, what and how decisions are prioritised to ensure IS resilience. To our knowledge there are no empirical validation of Weill's IT governance framework in the context of IS resilience planning, this will be an important contribution of this research.

## 2.12 COBIT and ITIL

Next we will discuss briefly one framework that has been widely adopted by large firms for IT governance and IT controls is COBIT (Control Objectives for Information and Related Technology) (Gelinas, Dull, & Wheeler, 2012).

COBIT definition for control is:

*“The policies, procedures, practices, and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that*

*undesired events will be prevented or detected and corrected”* (Gelinas, Dull, & Wheeler, 2012).

COBIT was developed by the IT Governance Institute to provide guidance to managers, users and auditors on the best practices for the management of information systems. According to COBIT, the IT resources which includes applications, information, infrastructure and people) must be managed by IT control processes to ensure that an organisation has the information it requires to achieve its goals. COBIT thus supports IT governance by providing a framework to ensure:

- IT/IS is aligned with the business
- IT/IS enables the business and maximises benefits
- IT/IS resources are used responsibly
- IT/IS risks are managed appropriately

COBIT's IT control processes are grouped into four main categories: (1) Plan and Organise, (2) Acquire and Implement, (3) Deliver and Support, and (4) Monitor and Evaluate. Within the Plan and Organise domain there are processes to develop strategy and tactics for understanding an organisation's IT strategy. Under 'Deliver and Support' Domain in COBIT it clearly states that in addition to managing IT operations, the IS function must ensure that IS resources are operational and secured. Ensuring continuous service is an important aspect of this process. The control plans under this process are directed at potentially catastrophic disruptions of business processes that could imperil the organisation's very survival (Business Continuity Institute, 2012). Many scholars has stated that continuity planning is a vital requirement and highlighted that organisations which experience a disruption and do not have

a disaster recovery plan and business continuity plan in place will fail eventually (Maurer & Lechner, 2014; Zheng et al. 2013).

To complement the IT governance framework Control Objectives for Information and related Technology (COBIT) provides for 34 identified IT processes and their corresponding high-level control objectives and management guidelines for IT decision makers. Control objectives can help support IT governance within an organisation. COBIT's management guidelines also includes the maturity models for each of the 34 IT processes (Haes & Van Grembergen, 2004). The first process identified by COBIT is “define a strategic information technology plan.” This process is vital to ensure strategic alignment. Different maturity levels are prescribed, for example, maturity level 1 requires that the need for IT strategic planning is known by IT management but there is no structured decision-making process. Whereas, to achieve highest maturity level 5, IT strategic planning should be a documented and living process, continuously considered in business goal setting and resulting in discernible business value through investments in IT. High level control objectives can be implemented through the use of the IT infrastructure library (ITIL). Thus, COBIT's control objectives tell the senior executives what to do while ITIL explains how to do it. But it is important to remember that having a high-level IT governance model does not automatically imply that IT governance is working in reality in the organisation.

### **2.13 Leadership**

An important characteristics of resilient organisations is the nature of their leadership (McManus et al. 2008). Leadership is so important that Penrose (2000) argue that in time of crisis an organisation with a great crisis response plan but poor leadership will perform poorly than an organisation that has great leadership but has an imperfect crisis



response plan. Penrose (2000) put leadership before crisis response plan. He emphasised that leadership during crisis is not only about making decisions. Leaders must lead from the front and should convey a sense of hope, optimism, opportunity, establish an inspiring vision, and assume the role of chief public relations officer by successfully communication with various stakeholders (Penrose, 2000). Penrose (2000) pointed that in many cases, the crisis might never occur or the impacts could be considerably limited if the organisation had more resilient leadership that is both inspiring and grounded in reality.

## **2.14 Culture**

Organisational culture is another crucial factor in effective decision making under crisis situation (Mitroff, 1988). Mitroff (1988) suggests that inflexible, hierarchical organisations with poor intra-organisational communication are more crisis-prone. He also emphasised that a noteworthy characteristic of crisis-prone organisations is the bent towards denial, known as head-in-the-sand culture. This head-in-the-sand culture according to Mitroff (1988) is ‘one of the most significant barriers to effective crisis management’. In order to overcome this culture of rejection, organisational leadership should recognise that not only that crises can happen to them but also are plausible to happen to them. Crichton (2006) suggests that crises are unavoidable for large complex organisations primarily because of the complexity in value-chain.

The level of planning for disasters has a direct relation on business survival following a disaster for small businesses (Crichton, 2006). As Penrose (2000) warn us, ‘smaller, lesser-known companies must heed the fact that 80% of companies without a comprehensive crisis plan vanish within 2 years of suffering a major disaster’.

Blake (1994) identifies that organisations are required to change their attitudes, values and behaviours, significantly all of them are characteristics of an organisation's culture. Blake (1994) identifies that it is evident that the large organisations will have an organisational culture to address crisis. Culture is predominant and as explained by him "...organisational culture can be seen as an expressive social tissue', and much like tissues in the human body, it binds the bones of organisational structure to the muscles of organisational processes". In essence, culture represents the 'life force' of the organization, the 'soul of its physical body'. Strong proactive culture is associated with superior performance and a critical aspect of resilient organisation (Ghobadian & O'Regan, 2006).

### **2.15 Crisis Management and Top Management Responsibilities**

The head of the IT function in many large organisations is the CIO. The responsibilities of the CIO are quite wide, including knowledge of technology, business and people management (Weiss & Anderson 2004). The CIO also provides leadership in IT governance (Rau 2004). Chun and Mooney (2009) conducted a survey of CIOs in the USA, and found evidence of three capabilities that CIOs most need in their job. These are relationship building, business systems thinking, and leadership. Thus, leadership has been recognized to be an important skill for CIOs. Leadership is, in particular, important during changing times when the organization and processes are in a flux, because it is precisely those times that the staff are most troubled and stressed in their jobs. Thus, CIOs should be competent in leading the staff of their organisations and supporting them in the recovery effort during and after the crisis has struck.

The CIO role marks a shift in historic approaches to IS management, which often viewed the IS manager as a functional line manager and technical expert (Applegate & Elam,

1992). However, as IS evolved to play a more strategic role, an evolution in the CIO role occurred. This evolution has been described as a movement from ‘backroom to boardroom<sup>1</sup>’ where the CIO is elevated to the level of other executives such as marketing, finance, manufacturing, human resources, and operations (Romanczuk & Pemberton, 1997). However, the CIO position is not a simple one. The CIO must deal with strategic business issues alongside the challenges of technology management (Watson, Kelly, Galliers & Brancheau, 1997). The CIO needs to plan strategically for IS and align IS priorities with the strategic information needs of the organisation whilst also ensuring continuity of IS services, infrastructure and application provision. CIOs operate in an environment where past practices have little bearing on future success (Gartner, 2007), and where organisational context still causes wide variations in management role, reporting levels, and nature of interactions with other executives (Grover, Jeong, Kettinger & Lee, 1993).

In a study of CIO effectiveness in the healthcare industry Smaltz, Sambamurthy, and Agarwal (2006) found six prominent roles for the CIO. Those roles are: “business strategist, integrator, relationship architect, utility provider, information steward, and educator” (Smaltz, Sambamurthy, & Agarwal, 2006). As they explained, the utility provider and information steward roles relate to the classic information technology (IT) responsibilities of providing computing services and providing appropriate access to and protection for information resources. The business strategist, integrator, relationship architect, and educator roles are focused less on the technology and more on the business and the effective utilization of information technology. These roles are growing in importance in many organisations. Weiss and Anderson interviewed 8 CIOs, 11 VPs of IT, and 75 IT staff members from several different Fortune 500 companies (Weiss & Anderson, 2004). They concluded that the work of

IT leaders has become more strategic and enterprise focused rather than maintenance and functional area focused. Polansky, Inugani, and Wiggins (2004) interview CIOs in leading global organisations and concluded that “the role of the CIO is moving from one of technical implementation to strategic planning and from reactive support of business needs to driving innovation and competitive advantage.”

Literature on CIO leadership has focused on understanding the leadership roles that CIOs need in their work during stable times, not crisis situations. These leadership roles revolve around communications and relationship building (Earl & Feeny 1994, Feeny & Willcocks 1998, Feeny et al. 1992, Grover et al. 1993, Stephens et al. 1992), strategic, visionary and entrepreneurial leadership (Applegate & Elam 1992, Chatterjee et al. 2001, Feeny & Willcocks 1998, Grover et al. 1993, Karimi et al. 1996, McLean & Smits 2003, Ross & Feeny 2000, Smaltz et al. 2006), and issue rather than people management roles such as technology, resource, operations and supplier management roles (Applegate & Elam 1992, Chatterjee et al. 2001, Earl & Feeny 1994, Feeny & Willcocks 1998, Grover et al. 1993, Karimi et al. 1996, McLean & Smits 2003, Ross & Feeny 2000, Smaltz et al. 2006, Stephens et al. 1992). Although people leadership aspects such as communications, relationship building and visionary are mentioned, these aspects are discussed mainly in relation to other organisational functions, not the CIOs’ decision priorities in the IT function.

As mentioned earlier, it is worth noting that decision functions in large organisations can be delegated in two general ways : (1) joint delegation to several agents (as in a committee), or (2) segregating and delegation of parts to different agents (as in giving sole responsibility of IS resilience to CIO). As preparing for IS resilience is a complex, multi-dimensional organisation wide, deep impact activity hence some organisations will rely on

decentralised decision making. Rather than relying on a single person (CIO) a small team of knowledgeable and experienced managers (members of C-Suites) may work together to ensure IS resilience by forming a “resilience committee”. Because of the importance of specific knowledge about particular area within the organisation – knowledge that is costly to transfer among agents- it is efficient for the teams in large organisations to make important decisions locally (Fama & Jensen, 1983). In such cases decision control may take place within team where interaction and mutual monitoring are heaviest. After making decisions the committee can report it back to board of directors at a regular interval for additional decision control.

### **2.16 Decision-Making Under Uncertain Situation**

As noted before, necessity to make decisions in fast changing situations along with incomplete information, ambiguity and uncertainty are characteristics of crises (Vargo & Seville, 2011). Decision makers under less than ideal circumstances and under stress, which may shift their focus to ‘short-range’ issues at the expense of ‘long-range’ outcomes (Vargo & Seville, 2011). Citing Bourgeois and Eisenhardt (1988), they prescribed that to make successful strategic decisions in crisis environments, organisations need to resolve a series of puzzles:

- to make strategic decisions carefully, but quickly;
- have a powerful, decisive CEO and a simultaneously powerful top management team;
- to seek risk while executing a safe, incremental implementation.

It is previously observed that successful organisations operating in fast changing environments find ways to put structure into a stream of unstructured decisions (Bourgeois, & Eisenhardt, 1988). They further observed that as the speed of environmental change speed up, effective managers deal with their extremely uncertain world by structuring it; using

rational techniques for searching and evaluating alternative actions (Bourgeois & Eisenhardt 1988). More importantly, successful and resilient firms are good at empowering their senior management team by delegating authority to implement strategy alongside functional responsibilities. Whereas, less successful and less resilient firms are more characterised by dictatorial and centralised decision hierarchies (Bourgeois & Eisenhardt 1988). Grover (1990) also suggests that decentralised decision-making process have a positive influence on the adoption and implementation of IS. Moreover, the management attitude towards IS risk is also crucial. The level of acceptable IS risk by top management could reflect in the decision-making process.

Other important lessons are, teams which are more successful in decision-making under fast changing environment attempt to mix strategic decisions with tactical plans (Eisenhardt 1989). Eisenhardt (1989) characterises fast decision makers as using more information and developing more alternatives than slower decision makers. Dealing with crisis situation and while analysing multiple options, decision makers focus on breadth-not-depth decision-making strategies, which laboratory studies have shown to be highly efficient when time pressure is high (Eisenhardt, 1989). It appears therefore that organisations must foster both structured and responsive decision-making approaches.

Snowden and Boone (2007) argue that in time of uncertainty, successful decision makers can tackle multiple demands and make variety of decisions. Snowden and Boone (2007) also mention that not all the decision makers will be successful in time of crisis if they continue to rely on traditional approach of leadership and decision making. It is often believed that an external environment exhibits some level of prediction and stability. This encourages managers to develop solution that fits in all situations. However, in reality sudden changes in

circumstances make the environment more complex and the fundamental assumption of simplification fails (Snowden & Boone, 2007). Snowden and Boone (2007) propose a framework called Cynefin (pronounced ku-nev-in, is a Welsh word that signifies the multiple factors in our environment and our experience that influence us in ways we can never understand) to see real-world problems from a new lens. The Cynefin framework aids decision makers determine the central operational context so that they can make appropriate choices.

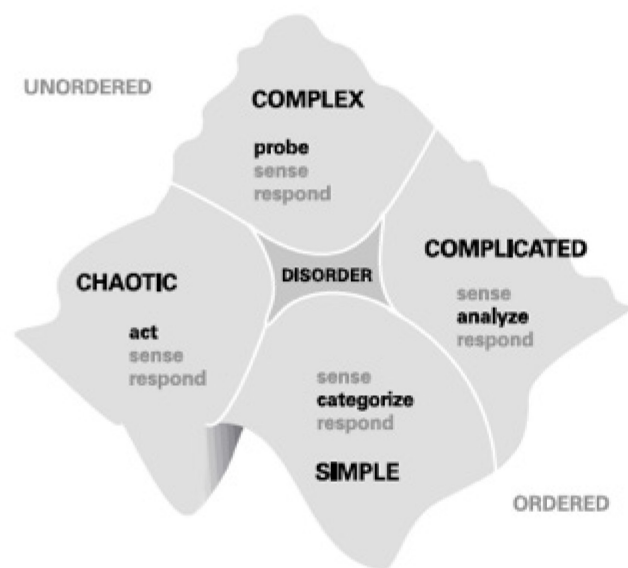


Figure 3 : Cynefin Framework (Snowden & Boone, 2007).

The Cynefin framework (Figure 3) proposes five dimensions and as proposed by the framework each domain requires different actions. The simple and complicated contexts assume an ordered universe, in which a right answer can be derived based on the facts and a predictable cause-effect relationship exists. Complex and chaotic contexts are unordered and as suggested by (Snowden & Boone, 2007), there is no direct relationship between cause and effect. For decision makers it is a very challenging situation and they rely on novel solutions based on emerging patterns. The ordered world represents fact based management whereas

unordered world represents pattern based management. The fifth dimension, known as disorder, refers to circumstances which are uncertain and unclear to categorise as other four (Snowden & Boone, 2007).

The decision-making process, which involves multiple players, having their own self-interest, imposes greater challenge for leaders to find out the best possible solution. In this research, two contexts, complex and chaotic domains, of Cynefin framework will be applied. IS resilience decision making like most other corporate governance decision making is often made in stressful, uncertain, complex and somewhat compromised settings. Thus, this research will investigate the decision-making process in a complex and chaotic situation, which is associated with the unordered domain in figure 3.

### **2.17 Risk Preferences and Prospect Theory**

Numerous models describe decision-making under ambiguity and risk. Most of these models focus on either the dispositional characteristics of individuals (Waller 1988) or the characteristics of the situational context (Kahneman & Tversky 1979). The ‘dispositional view’ suggests that risk preference is a personality trait that remains constant over time and context (Waller 1988). Based strictly on dispositional characteristics, risk-seeking individuals should prefer risky choices, and risk-averse individuals should prefer riskless choices. In context of this research the risk preferences of CIOs and other important decision makers should influence IS resilience decisions. So, we would expect that risk-seeking decision makers at Jade will prefer risky choices, and risk-avoiding decision makers will prefer risk-less choices. Other research finds that: ( 1) risk preferences can change with decision context, and ( 2) risky choices are not solely a function of dispositional characteristics (Kahneman & Tversky 1979). This is one fundamental premise of prospect theory — “individuals seek risk



in loss decision domains and avoid risk in gain decision domains” (Kahneman & Tversky 1979). Kahneman and Tversky's (1979) prospect theory is a widely accepted behavioural model of risky decision making. Prospect theory suggests that individuals avoid risk when they perceive the current state to be positive (a gain decision domain), and individuals seek risk when they perceive the current state to be negative (a loss decision domain). Determination of the gain or loss decision domain depends on an individual's subjective reference point. The reference point is determined by comparing the current state to some prior state, or, by comparing the current state to the state of a peer group (Kahneman & Tversky 1979).

Tversky and Kahneman (1979) describe situations where a decision maker's current state places the decision maker in a gain or loss domain. For example, they describe this scenario: "Consider a person who has spent an afternoon at the race track, has already lost \$140, and is considering a \$10 bet" (Tversky & Kahneman 1979). The gambler has fallen behind an initial reference point of no losses and is now in a loss domain. The new reference point is a loss of \$140, and the gambler will seek out long-shot bets to return to a neutral reference point. Conversely, a gambler who had prior winnings would be above a neutral reference point and would avoid long-shot bets. Tversky and Kahneman (1979) are asserting that the person's current situation causes them to frame the betting decision a certain way.

We can describe a similar scenario in context to our research. If we consider a normal situation as a gain domain for an organisation then during the time of crisis due to the obvious effects of crisis the same company will operate in a loss domain. The intention of IS resilience planning is to minimise the impact of losses that may be caused by crisis. So, in other words, using resilience planning, organisations will attempt to shift the crisis related losses to

the new reference point in loss domain and the decision makers will seek out for strategies to mitigate crisis and return to a neutral reference point.

While research demonstrates people adopt different decision behaviours under gain and loss domains (Kahneman & Tversky 1979), we know of no research that examines how CIOs and other key decision makers prioritise IS resilience decisions based on a decision domain. Do CIOs and other key decision makers recognize the decision domain and use this information in prioritisation of decisions? In this study we will test CIOs along with other key decision makers to make decision based in a loss decision domain. The concept that decision domains influence CIO's and other key decision makers' decisions is a novel application of prospect theory that is not investigated in prior research in Information Systems (IS).

The key findings of literature review may be summarised as follows:

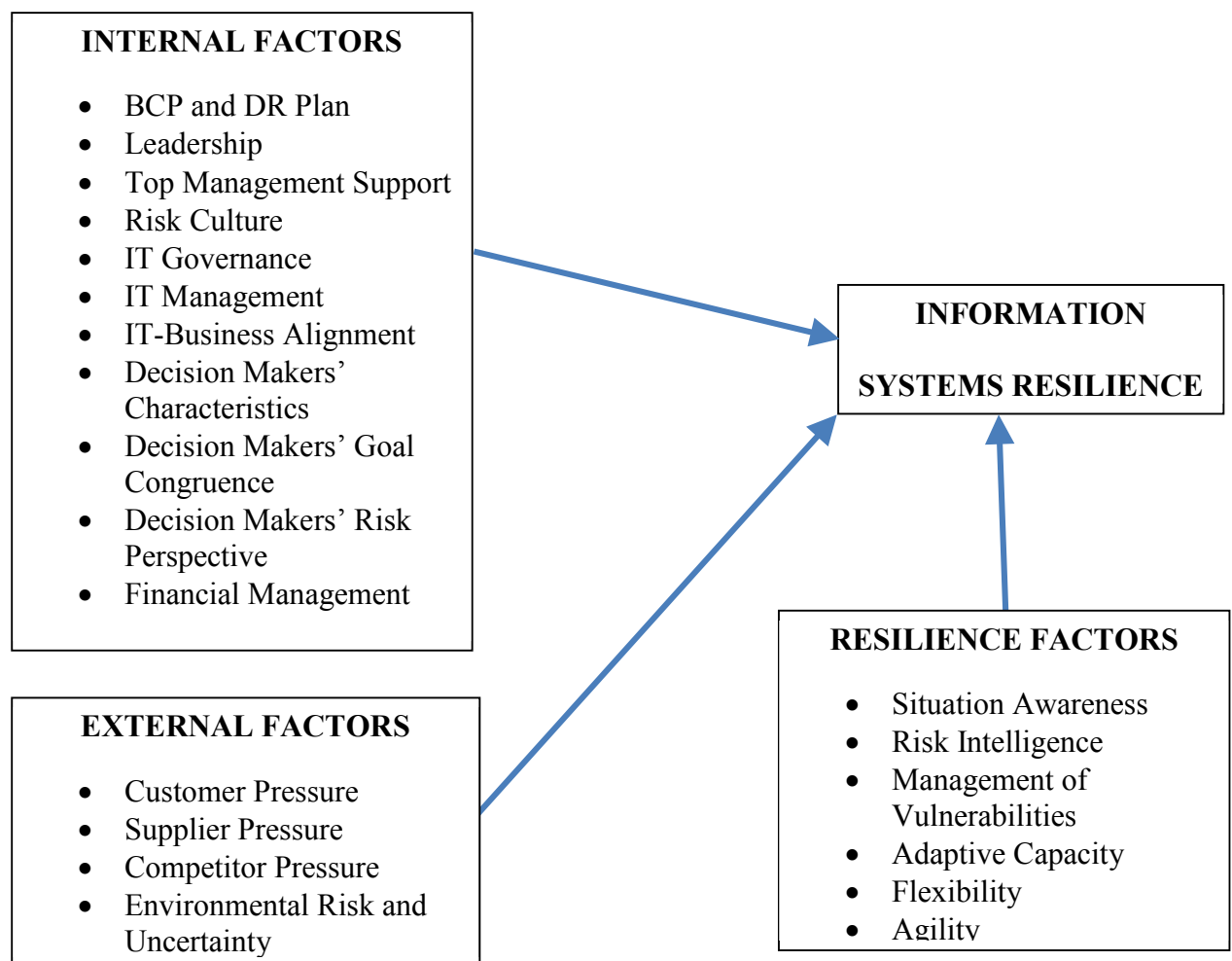
- Organisations increasingly rely on complex IS and digital platforms to manage their businesses, which require IS to operate reliably under a variety of adverse circumstances.
- To date, there has been no systematic examination of how IS resilience planning decisions are made.
- Agency theory has demonstrated significant predictive power with respect to the decision-making of owners and managers by its proposition of the principal-agent relationship dynamics. Agency theory assumes that there is a lack of goal congruence between the principal and agent and that it is costly or difficult to confirm the agent's actions (Eisenhardt, 1989). In other words, left to their own procedures, the agents will prefer different options to those that would be chosen by the principals. The agents would make decisions and follow courses that further their own self-interest as opposed

to that of the principal. However, Agency theory does not deal directly with IT-related decision-making or risk distribution.

- Peter Weill's IT governance framework explains how decision rights and responsibilities are distributed within the IS function in organisations. Agency theory and Weill's IT governance framework are compatible with regard to both decision rights and decision responsibilities.
- Attributes of IS resilience as identified during literature review are (1) Overall Situation Awareness, (2) Management of Vulnerabilities, (3) Adaptive Capacity, (4) Risk Intelligence, (5) Flexibility, (6) Agility, (7) Planning, (8) Leadership, (9) Risk Culture, (10) IT and Business Alignment, (11) Communication, (12) IT governance, (13) Top Management Support, (14) Organisational Decision Making and (15) Top Management Team's IS Knowledge.
- Prospect theory predicts that people adopt different decision behaviours under loss and gain domain. In other words, individuals seek risk in loss domain.

### 3. CONCEPTUAL RESEARCH MODEL

A conceptual framework of determinants of IS resilience, and therefore what ought to be the decision priorities for one who is responsible for IS resilience, is presented in Figure 4. Internal and external factors presented in the above framework of IS resilience for organisations are derived from the literatures discussed in the previous section. In the context of this research, the model provides a guide for the development of instrumentation, and interpretation of the results.



*Figure 4. Preliminary IS Resilience Conceptual Framework*

## 4. RESEARCH METHOD

### 4.1 Q-Methodology and Q-Sort

Essentially, this research is studying the decision process of senior executives decision priority in context of IS resilience. Which involves the prioritisation of different decisions related to IS resilience in uncertain situation. Q-methodology provides a groundwork for the systematic study of subjectivity. In this methodology a participant is presented with a set of statements on a topic and is asked to order them in rank. This operation is known as Q-sorting. A Q-sort requires the participant to sort through a field of statements that represent the concourse, and to classify those statements into a quasi-normal distribution, typically between "most important" and "most unimportant", or "most desirable" and "most undesirable". In doing so, the Q-sort captures the participant's priorities with respect to the concourse, and operationalizes their unique perspective. The Q-methodology is appropriate for situations where the goals are exploratory, a rich and interpretive understanding is desired, and there is small number of participants. Therefore Q-methodology was employed in accordance with the goals of this study to identify IS resilience planning priorities in organisations. According to Brown (1980) utilizing the Q-methodology involves the adoption of three things: its directorial viewpoint of conserving operant subjectivity, the guidelines for instrument development and measurement using the q-sort, and a specialized centroid factor extraction technique known as "q-factor analysis". The preservation of operant subjectivity may well be described as the principle of allowing the subjects to speak in their own voice (Brown, 1980). The idiographic nature of the Q-methodology makes it appropriate for this study.

The fundamental steps of the Q sorting procedure are as follows. A heterogeneous set of items (called a Q sample) is drawn from the concourse. A group of respondents (P set)

is instructed to rank-order (Q sort) the Q sample along a standardized range according to a specified condition of instruction. Participants do this according to their own 'psychological significance'. The resulting Q sorts are submitted to correlation and factor analysis. Interpreted results are factors of 'operant subjectivity' (Brown, 1980).

Concourse theory is a theory of communicability which proposes that people "operate" within a universe of possible thoughts, ideas, feelings, and related referential material (Brown, 1980; Klaus, Wingreen, & Blanton, 2010; Stephenson, 1986a & 1986b). The universe of possibilities for any given topic is a 'concourse', and each participant possesses a unique 'perspective' of the concourse that is reflected by their own personal prioritization of the content of the concourse. Stephenson (1986a & 1986b) relied on the philosophy of William James (1891) to develop Concourse theory. James (1891) links a person's thinking process to a bird flying between perches – the bird is either flying or perched but both are complementary elements of the same process. James argued that though cognitive process is a flux but it is also differentiated: the bird's life is a seamless unity but it also contains two different kinds of activity, flying and perching. Similarly, a person's transitory thought process periodically perches on substantive thoughts, but both are complementary elements of the same thinking process. Complementary nature of substantive and transitory thought is fundamental to the principle of complementarity in quantum theory as well as in Q-Methodology.

Concourse theory prescribes Q-methodology as the principal means of operationalizing a concourse, and the perspectives of people with reference to the concourse. To operationalize the person's unique perspective of a concourse, Q-methodology proposes the Q-sort and Q-factor analysis (Stephenson, 1986 - 1988; Wingreen, Lerouge, Blanton, 2009; Wingreen et al., 2005). Therefore, concourse theory, Q-methodology, and the Q-sort are also

appropriate to operationalize the decision priorities of senior executives in organisations, since in their planning and decision making, they also operate within a "concourse" of criteria related to IS resilience.

In summary, as pointed out by Wingreen et al. (2009), Q-methodology includes a quantitative analysis that is lacking in most qualitative and interpretive methods (Stephenson, 1986a, 1986b, 1987, 1988). However, it upholds the rich story told in the own language of its participants, a feature generally found with case-based research or other grounded theory methods (Eisenhardt, 1989). Wingreen et al. further added that Q-factor analysis generates empirically derived factors and factor scores that associate each person with each factor/type revealed in the analysis. Q-factor analysis is an improvement over the descriptive and non-parametric statistics that are generally associated with case-based research and other grounded theory methods. This is a significant point, since it enables Q-methodology to generate the same level of richness that is possible with case-based research while working with the larger sample sizes (sometimes referred to as P-sets in Q-methodology) associated with empirical field research. In other words, Q-methodology allows researchers both to make generalizations comparable to those obtained in empirical field research, such as surveys, while maintaining a level of phenomenological richness that is comparable to case based interpretive research (Wingreen et al., 2009).

#### **4.2 Reliability and Validity in Q-methodology**

Reliability and validity do not have the same standing in Q-methodology as they do in r-methodological research. In r-methodological research, where objectivity is highly valued, objective measurements are critical to accomplish the goals of the research, and therefore the measurements must be accurate and error-free (reliable), and must really measure

what it is supposed to measure (valid). In Q-methodology, since analysis of the person's subjective viewpoint is the goal; reliability and validity apply to the person rather than the measurements. The same questions about reliability and validity simply have no meaning when applied to the person's subjective viewpoint (Dennis, 1993). As Brown (1980) argues, "there is obviously no right or wrong way to provide 'my point of view' about anything". Similarly, by what standard shall we validate a participant's subjective viewpoint, and what does it mean to ask whether a participant's subjective viewpoint is "error-free"? Thus, Lincoln and Guba (1985) proposes that if a participant's subjective viewpoint is by definition valid, and since there can be no validity without reliability, a demonstration of the former is sufficient to establish the latter.

Nevertheless, there are some areas Q-methodologists observe in the interest of "due diligence" (Wingreen et al., 2009). There is a kind of response bias that is peculiar to Q-methodology in which the respondent sorts the q-statements in the order they were presented, which in the context of this study is an indication that the respondent was not thoughtfully engaged with the q-statements while performing their q-sort. None of the Q-sorts fall under this criteria for this research.

#### **4.3 Instrument Development**

Two set of instruments were developed as part of this research. The first instrument is designed to measure the risk preferences of the CIOs and senior management team members and the second instrument was the Q-sort questionnaire which is developed to understand the CIO decision priorities related to IS resilience in a crisis situation.

Description of First Instrument: The CIO and key decision makers risk preference was measured using a lottery problem from (Kahneman & Tversky, 1979) and an alternative



risk preference measure questionnaire. Risk preference measures were collected at the beginning of the experiment.

An example of the scale used in the experiment is as follows:

As one of the top managers of my organisation ....	Strongly Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Strongly Agree
I believe that greater risks are worth taking in a normal situation.					
I believe that greater risks are worth taking in an uncertain situation.					

Information obtained from the risk preference questionnaire will indicate whether the decision maker's decision changes in a gain or loss decision domain as described in prospect theory. An example of the lottery problem question used to understand the overall risk orientation of the CIO in the experiment is as follows:

A. You have a choice between the following two options:

1. A sure gain of \$750.
2. 40% chance to gain \$2000 and 60% chance to gain nothing.

Please indicate which option you will choose.

#### 4.4 The Q- Sample

The q-sample consist of statements from 1) review of the literature, 2) conversations and interviews with people who participate in the concourse, and 3) input from domain experts

about the content of the sample of Q-statements. The instrument contains thirty seven (37) statements related to senior executive decision priority on IS resilience context, as noted below.

<b>Resilience Statements</b>	<b>Weill's IT Decision Domain</b>	<b>IS Resilience Factors</b>
Information Systems (IS) Disaster Recovery plans informed by understanding of underlying causes of vulnerability and other factors outside organisation's control.	IT Architecture	Disaster Recovery and Situation Awareness.
Organisation Information Systems (IS) Continuity plans, developed through participatory processes, put into operation and updated periodically.	IT Principles	Business Continuity Planning and Management of Vulnerabilities..
Organisation's Information Systems (IS) resilience plan shared with all suppliers.	IT Principles	Communication, Relationship Management and Risk Intelligence.
Organisation hazard/risk assessments carried out which provide comprehensive picture of all major hazards and risks faced by organisation (and potential risks).	IT investments and priorities, IT Infrastructure Strategies	Risk Management, Situation Awareness and Risk Intelligence.
On-going monitoring of hazards and risks and updating of plans.	IT Principles	Disaster Recovery and Business Continuity Planning. Commitment to Risk Management and Monitoring. Adaptive Capability.
Organisational vulnerability and capacity assessments carried out which provide comprehensive picture of vulnerabilities and capacities.	IT Investment and Prioritisation	Business Impact Analysis, Organisational Culture and Risk Intelligence.
Resilient and accessible critical facilities (e.g. back-up systems, redundancy of data).	IT Architecture and Infrastructure Strategies	Infrastructure and Technical Capability, BC and DR Planning. Adaptive Capacity.

Top management support and commitment to Information Systems (IS) resilience.	Critical for effective IT Governance	Top Management Support. Organisational Culture. Agile and Adaptive Capacity.
Information Systems (IS) resilience can provide an organisation with an edge over its competitors.	IT Principles	Leadership, TMT's IS Knowledge. Agile.
Our competitors are developing and enhancing their Information Systems (IS) resilience capabilities.	IT Principles	Competitor Pressure, Organisational Culture and Situation Awareness.
A sound Information Systems (IS) resilience plan will help us to win more business contracts.	IT Principles	Financial Management and Situation Awareness.
A sound Information Systems (IS) resilience plan will help us to pay lesser insurance premium.	IT Principles	Financial Management, Organisational Culture and Situation Awareness.
A sound Information Systems (IS) resilience plan will help our organisation to make more efficient use of resources.	IT Principles	IS Planning, Resource Capability and Adaptive Capacity.
Long-term Information Systems (IS) Resilience, Business Continuity, Disaster recovery justification and planning.	IT Infrastructure and IT Investment and Priority	Leadership, TMT's IS knowledge. Risk Intelligence.
Competitor Analysis - Survive disruptions that your competitors cannot.	IT Principles	Learnability and TMT's IS knowledge. Agile, Flexible and Management of Vulnerabilities.
Setting up information disaster recovery system (e.g., disk redundancy, backup facility).	IT Architecture, IT Infrastructure and IT Investment and Priorities	Infrastructure and Technical Capability, DR Planning. Management of Vulnerabilities and Adaptive Capacity.
Study resilience strategies of competitors.	IT Principles	Learnability, Organisational Culture, Risk Intelligence.

Select suppliers with robust resilience plan.	IT Infrastructure Strategies and IT Principles	Business Continuity Planning, Risk Management Strategy. Risk Intelligence.
Use Information Systems (IS) network to communicate with the customers.	IT Infrastructure Strategies	Communication and Agile.
Use Information Systems (IS) networks to connect to supplier's databases.	IT Infrastructure Strategies	Communication and Connection. Agile.
Use cloud computing to back up organisational data.	IT Principles and IT Infrastructure Strategies	TMT's IS Knowledge and Technical and Infrastructure Capability. Management of Vulnerabilities.
The level of customer involvement in preparing resilience, business continuity and disaster management plans.	IT Principles and IT Infrastructure Strategies	Organisational Culture, TMT's IS Knowledge and Leadership. Risk Intelligence.
The extent of follow-up with customers for feedbacks.	IT Principles	Communication and Risk Intelligence.
The level of supplier involvement in preparing resilience, business continuity and disaster management plans.	IT Principles	Organisational Culture, TMT's IS Knowledge and Leadership. Situation Awareness.
Ensuring data security	IT Principles and IT Architecture	Trust, Organisational Culture, Customer Pressure. Adaptive Capacity.
Receiving reliable and consistent services from Suppliers	IT Principles	Trust, Organisational Culture. Agile.
Providing reliable and consistent services to customers	IT Principles and IT Infrastructure	Trust, Organisational Culture, Customer Pressure. Agile, Adaptive Capacity and Management of Vulnerabilities.
Capability for disaster recovery	IT Principles and IT Infrastructure	Infrastructure and Technical Capability. Management of

		Vulnerabilities and Adaptive Capacity.
Providing the organizational units with information for 24 hours a day, 7 days a week	IT Principles	Infrastructure and Technical Capability, BC Planning, Customer Pressure, Competitor Pressure. Agile and Management of Vulnerabilities.
Understanding the strategic priorities of top management	IT Principles	Aligning IT with Business Strategy. Adaptive Capacity and Agile.
Aligning Information Systems (IS) strategies with the strategic plan of the organisation	IT Architecture	Organisational Culture and Senior executives IT knowledge. Adaptive Capacity and Management of Vulnerabilities.
Adapting technology to strategic change	IT Architecture	TMT's IS Knowledge, Aligning IT with Business Strategy. Agile and Adaptive Capacity.
Information Systems (IS) resilience plan that is well defined and structured	IT Principles	IS Planning, Organisational Culture. Management of Vulnerabilities and Situation Awareness.
Information Systems (IS) resilience plan that is flexible and adaptable	IT Principles	IS Planning, Organisational Culture, Flexible, Management of Vulnerabilities and Situation Awareness.
Ability to identify key risks	IT Principles and IT Architecture	TMT Characteristics – Risk Averse or Risk Tolerant (prospect theory).  Risk Intelligence and Situation Awareness.
Ability to anticipate surprises and crises	IT Principles	TMT Characteristics – Risk Averse or Risk Tolerant (prospect

		theory). Risk Intelligence.
Committed, effective and accountable leadership of Information Systems (IS) resilience planning and implementation.	IT Principles	Leadership and Agile.

*Table 2. Factors affecting IS resilience, Weill's IT Decision Domain and related Q-Statements.*

#### **4.5 Description of Second Instrument**

The Q-sort instrumentation, a set of 37 Q-sort statements, was developed according to the guidelines delineated by previous research (Brown, 1980; Stephenson, 1986a, 1986b, and 1986c). A set of Q-sort statements should represent the concourse of interest in the same way that a sample of people should represent the population in a classical correlational study. Therefore, certain prescribed guidelines are adopted in the selection of statements so as to achieve the highest probability of "representativeness" of the domain of the concourse: 1) review of the literature, 2) conversations and interviews with people who participate in the concourse, and 3) input from domain experts about the content of the sample of Q-statements (Brown, 1980; Dennis, 1988).

Furthermore, if there are areas of theoretical interest, as there are in this research, then a "structured q-set" may be developed, which balances the number of Q-statements in each theoretical category, in much the same way as experimental participants are assigned to groups for balanced experimental designs in classical experimental research (Watts and Stenner, 2012). To accomplish this, we selected statements from figures 1 and 2 to represent the various dimensions of IS resilience which should be reflected in the decision priorities of CIOs and other key decision makers. These items were then coded according to Weill's IT domain and various IS resilience factors as identified in literatures (see table 2). Therefore, the final set of

37 items was both representative of the larger concourse and well-balanced with regard to all the theoretical categories of interest in the current research (Appendix A shows the Q-sorts used in the questionnaire).

#### **4.6 Pilot Test**

In order to ensure content validity of our instruments we conducted a pilot test. As part of this pilot study CEO owner-managers of local SMEs and domain experts were recruited to assist as evaluators with the item selection phase. Following the guidelines for instrument development, feedback from the evaluators was incorporated into the Q-statement and Q-Sort instrumentation (Stephenson, 1986 - 1988; Wingreen, Lerouge, Blanton, 2009; Wingreen et al., 2005). After several iterations of the instrument development guidelines, the evaluators confirmed that the instrument is ready and should function as intended. We then approached seven (7) CEO owner-managers of local SMEs, who provided their own Q-sorts for the purposes of testing the statistical properties of the Q-sort set and also evaluated the Q-Sort instrument. Furthermore, in order to test the theoretical structure incorporated into the Q-set, a CIO of a local public institution was recruited to provide his own Q-sort. Agency theory predicts that the IT manager of a public institution should have very different IS resilience planning priorities than CEO owner-managers of SMEs, and these priorities should manifest themselves by the selection of Q-sort statements from different theoretical categories from the structure of the Q-sort set. The data gathered was analysed using the PQ-method software that is commonly used in Q-methodology research (Wingreen et. al. 2005). Our initial research was successful, therefore, the Q-methodology was adopted and employed in accordance with the goals of this research.

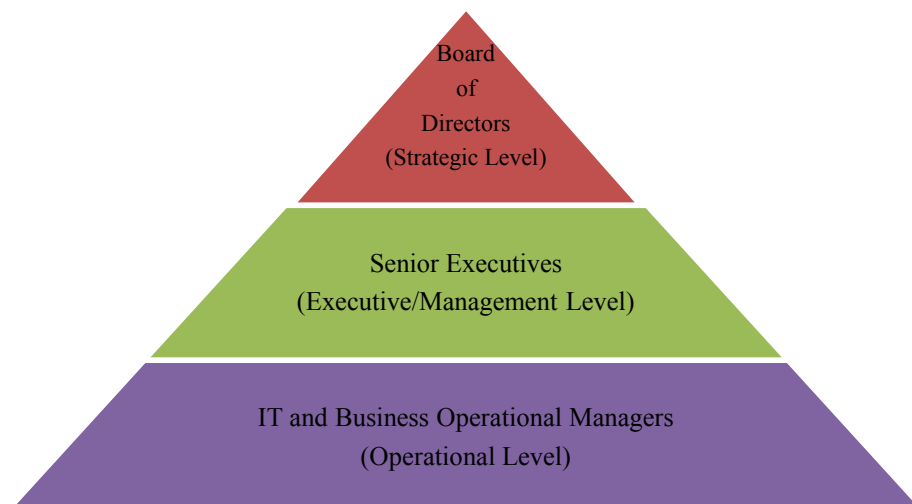
#### **4.7 A Brief Introduction to Jade Software Corporation**

Jade Software Corporation Limited was founded in 1978 and is head quartered in Christchurch, New Zealand. Jade works with leading companies around the world to solve complex business problems through the design and delivery of innovative software solutions. Jade is a large organization with 45 major partners, and offices in the United States, the United Kingdom, the Middle East, the Netherlands, Indonesia, New Zealand and Australia. The company operates three main lines of business: Jade Solutions: custom software development and support; Jade Technologies: JADE programming language and database platform; Jade Logistics – Terminal Operating System for mixed cargo shipping ports.

Jade experienced a number of challenges as a result of the Christchurch earthquakes. At the time of the disasters, the communications network and electricity cuts were problematic, with personal employee issues following in the days after the earthquakes. Jade had in place a robust and rehearsed IS resilience plan, had set up special control rooms, as well as establishing a task list and contact tree for emergencies. Therefore, Jade was prepared when the disaster struck. Jade's primary business operations are located within the disaster zone of 2010 and 2011 Christchurch earthquakes and as a result, suffered a perturbing blow to business operations. But, as they were well prepared, they quickly adapted to the changed environment and successfully met all contractual requirements throughout the crisis. One of most important aspects to understand resilience is to know how people learn to adapt and what happens when they stop learning from experiences (Kayes, 2015). However, in this context, what is absent is empirical research that shows how learning is sustained during crises and how lessons learned after a crisis actually make a difference later. As all the key decision makers at Jade have already experienced a crisis scenario, this issue will be addressed and will add realism to this study.



Top Management Team (TMT) is described as the link between the board of directors of a firm and the managers entrusted with the day-to-day functioning of the firm. Consistent with the description, Fama and Jensen (1983) have described them as the “apex of the firm’s decision control system”. Thus, TMT is an elite workgroup with a crucial role in firm’s decision-making and face complex, multifaceted tasks that involve both strategic and technical issues. TMT is responsible for not only decision-making but also for implementing and administering those decisions (Fama & Jensen, 1983). Jade has a committee that is responsible for risk management and IS resilience planning. The committee consists mostly of members of the executive management team responsible for the various areas of the company. They work together to ensure that all prospective risks are identified, mitigated, and planned for. TMT’s direct involvement and decision-making before, during and after the crisis will add realism to this study. As mentioned previously in the definition of IT governance, it is crucial to have the roles and responsibilities defined unambiguously for an effective IT governance framework. Figure 5 implies that different committees has different memberships and authorities at Jade.



*Figure 5. Three layers of IT Governance responsibility at Jade Software Corporation*

## 5. RESEARCH FINDINGS AND DISCUSSION

This section presents the research findings that were reached through analysis of Q-sort data. The Q-sort data was analysed using a centroid factor analysis, as suggested by prior research (Watts & Stenner, 2012). Two and three factor solutions were examined at first, however, since the three factor solution converged to a two-factor solution, there was no need to continue, and a two-factor solution was adopted. Jade's IS resilience committee, which constitutes of seven (7) c-suite executives are distributed in two types of decision makers – (1) business focused strategic decision makers (type 1) and (2) technical focused tactical decision makers (type 2) (refer to table 3). In this study our focus is to develop and validate an IT governance framework in context to IS resilience and to have a deep understanding of how decisions are made by the top management team to ensure IS resilience.

The 'Risk Preference' (first instrument) is designed to measure the risk perspective of decision makers and is based on Prospect theory. Prospect theory predicts that people adopt different decision behaviours under loss and gain domain. In other words, individuals seek risk in loss domain and will be risk averse in gain domain. During our interview we asked the senior executives to answer the risk preference related questionnaire and decision makers at Jade exhibit behaviours consistent with Prospect theory. So, the decision makers at Jade are not afraid to take risks in loss domain (in time of crisis).

Second instrument captures decision priorities of senior executives, table 3 reports that seven (7) senior executives can be distributed into two types and their respective positions in the organisation have also been outlined. The "Role" column reports how senior executives classified their roles as either technical or strategic, based on their position in the organisation.

There was 100% inter-rater agreement between the senior executives and the researchers for this classification.

<b>TMT Members</b>	<b>Type 1</b>	<b>Type 2</b>	<b>Role</b>
PRILO1	0.4621	<b>0.7737</b>	<i>Technical</i>
PRILO2	<b>0.6890</b>	0.2399	<i>Strategic</i>
PRILO3	0.5286	<b>0.5397</b>	<i>Technical</i>
PRILO4	0.1469	<b>0.8787</b>	<i>Technical</i>
PRILO5	<b>0.7222</b>	0.2998	<i>Strategic</i>
PRILO6	<b>0.7338</b>	0.3614	<i>Strategic</i>
PRILO7	<b>0.8741</b>	0.1662	<i>Strategic</i>

Table 3. Q-Factor Matrix of 2 Factor Solution

Table 4 reports the results of the factor analysis, which reveals two "types" of decision priorities. The factor scores are the factor Q-sort values for how each statement was prioritized on the Q-sort distribution by those who comprise that factor. The "rank" is the average ranking of that statement by those who represent that factor. The highest and lowest rankings are highlighted so as to illustrate the decision priorities that represent each type. Also, the statement numbers with asterisks (\*) denote distinguishing statements between two types. With these distinguishing statements we went back to Jade to interview the senior executives and find out the reason behind different priorities. A type is defined by both the high and low priorities as well as distinguishing statements, since both distinguish any given type from others, and therefore the analysis proceeds by interpreting and defining the types based on their respective priorities. As mentioned earlier, during the interview stage with the senior executives we asked them to categorise the Q-statements according Weill's IT decision domain by referring to the 'Key Issues for Each IT Decision Area (by Peter Weill)' questionnaire (please refer to

Appendix). There was 100% inter-rater agreement between the senior executives and the researchers for this categorisation.

Resilience Statements	No.	IT Decision Domain (by Peter Weill)	Factor Scores	
			<i>F1</i>	<i>F2</i>
Information Systems (IS) Disaster Recovery plans informed by understanding of underlying causes of vulnerability and other factors outside organisation's control.	1	IT Architecture	1	1
Organisation Information Systems (IS) Continuity plans, developed through participatory processes, put into operation and updated periodically.	2*	IT Principles	2	1
Organisation's Information Systems (IS) resilience plan shared with all suppliers.	3*	IT Principles	0	-2
Organisation hazard/risk assessments carried out which provide comprehensive picture of all major hazards and risks faced by organisation (and potential risks).	4*	IT investments and priorities, IT Infrastructure Strategies	3	1
On-going monitoring of hazards and risks and updating of plans.	5	IT Principles	1	0
Organisational vulnerability and capacity assessments carried out which provide comprehensive picture of vulnerabilities and capacities.	6*	IT Investment and Prioritisation	2	-1
Resilient and accessible critical facilities (e.g. back-up systems, redundancy of data).	7*	IT Architecture and Infrastructure Strategies	2	3
Top management support and commitment to Information Systems (IS) resilience.	8	Critical for effective IT Governance	2	3
Information Systems (IS) resilience can provide an organisation with an edge over its competitors.	9*	IT Principles	0	-2
Our competitors are developing and enhancing their Information Systems (IS) resilience capabilities.	10*	IT Principles	-2	0
A sound Information Systems (IS) resilience plan will help us to win more business contracts.	11	IT Principles	0	-2

A sound Information Systems (IS) resilience plan will help us to pay lesser insurance premium.	12	IT Principles	-3	-3
A sound Information Systems (IS) resilience plan will help our organisation to make more efficient use of resources.	13	IT Principles	-3	-3
Long-term Information Systems (IS) Resilience, Business Continuity, Disaster recovery justification and planning.	<b>14*</b>	IT Infrastructure and IT Investment and Priority	-2	2
Competitor Analysis - Survive disruptions that your competitors cannot.	15	IT Principles	0	-2
Setting up information disaster recovery system (e.g., disk redundancy, backup facility).	16	IT Architecture, IT Infrastructure and IT Investment and Priorities	3	2
Study resilience strategies of competitors.	17	IT Principles	-1	-1
Select suppliers with robust resilience plan.	<b>18*</b>	IT Infrastructure Strategies and IT Principles	-1	2
Use Information Systems (IS) network to communicate with the customers.	19	IT Infrastructure Strategies	0	0
Use Information Systems (IS) networks to connect to supplier's databases.	20	IT Infrastructure Strategies	-1	-1
Use cloud computing to back up organisational data.	21	IT Principles and IT Infrastructure Strategies	0	0
The level of customer involvement in preparing resilience, business continuity and disaster management plans.	<b>22*</b>	IT Principles and IT Infrastructure Strategies	-2	0
The extent of follow-up with customers for feedbacks.	23	IT Principles	-1	0
The level of supplier involvement in preparing resilience, business continuity and disaster management plans.	24	IT Principles	-1	-1
Ensuring data security	25	IT Principles and IT Architecture	1	0
Receiving reliable and consistent services from Suppliers	26	IT Principles	-1	-1
Providing reliable and consistent services to customers	27	IT Principles and IT Infrastructure	1	2

Capability for disaster recovery	28	IT Principles and IT Infrastructure	1	1
Providing the organisational units with information for 24 hours a day, 7 days a week	29	IT Principles	0	0
Understanding the strategic priorities of top management	30	IT Principles	0	0
Aligning Information Systems (IS) strategies with the strategic plan of the organisation	31*	IT Architecture	0	1
Adapting technology to strategic change	32*	IT Architecture	-2	0
Information Systems (IS) resilience plan that is well defined and structured	33	IT Principles	0	1
Information Systems (IS) resilience plan that is flexible and adaptable	34	IT Principles	0	0
Ability to identify key risks	35	IT Principles and IT Architecture	0	0
Ability to anticipate surprises and crises	36	IT Principles	0	-1
Committed, effective and accountable leadership of Information Systems (IS) resilience planning and implementation.	37	IT Principles	1	0

Table 4. Q-sort statements with their corresponding ranks and z-scores, statement numbers with asterisks (\*) denote distinguishing statements between Type 1 and Type 2

### ***Type 1: Business Focused Strategic Decision Makers***

Type 1 can be characterised as business focused strategic decision makers. According to Weill (2004) they are business monarchs and are more comfortable with IT principles and IT investment and prioritization types of decision making. They have high level enterprise wide views and clearly prioritised more strategic than technical type decisions which can be exemplified by these highly ranked statements: “Organisation hazard/risk assessments carried out which provide comprehensive picture of all major hazards and risks faced by organisation (and potential risks)” (rank 1) and “Organisational vulnerability and capacity assessments carried out which provide comprehensive picture of vulnerabilities and capacities” (rank 5). Both questions fall under Weill’s (2004) IT investment and priority category; hence,

they are more strategic than technical. Type 1 decision makers want more certainty around risks, as reflected by the statement of one of their executives, “a comprehensive picture is essential to foresee risks in order to manage them and ensure that correct risks are addressed”. When probed on another statement, “Organisation ISCP plans, developed through participatory processes, put into operation and updated periodically”, which was ranked (6) by type 1 whereas ranked (11) by type 2, we found that both types understand that this is important and existing plans need to be regularly audited, exercised and updated, that is what they do in practice also. Type 2 also mentioned that existing IS resilience plan requires to be updated regularly to reflect the changes in technology, business environment and customer priority changes. This statement falls under IT principles category, hence it makes perfect sense that why it is ranked high by Type 1 in compare to Type 2.

### ***Type 2: Technical Focused Tactical Decision Makers***

Type 2 can be characterised as technical focused tactical decision makers. According to Weill (2004) they are IT monarchs and are comfortable in IT architecture, and IT infrastructure strategy types of decision making. They are involved in implementation of high-level views and are responsible for implementing IS resilience and ensuring day to day operation of the organisation. This group clearly preferred technical priorities over strategic priorities, as exemplified by the high ranking they assigned to, “Select suppliers with robust resilience plan” (rank 6), which falls under both the IT infrastructure and IT principles categories, but received a low ranking from Type 1 (rank 27). When probed Type 2 decision makers said, “we [technical team] understand that in [regard to] hardware and infrastructure, if we do not get replacements on time, then we will end up with problems. It is critical for us”. On the other hand, Type 1 overestimates the independence of the firm. Another interesting

finding for Type 2 is related to, “Long-term Information Systems (IS) Resilience, Business Continuity, Disaster recovery justification and planning” (rank 5), which falls under both the IT infrastructure and IT Investment and Prioritisation categories. According to Weill (2004) both type 1 and type 2 should consider the statement to be important. Surprisingly, Type 1 ranked it 34 while Type 2 ranked it 5. When probed we found that according to Type 1, top level strategic type decision makers’, “IT changes too fast thus there is hardly any value in making a long term [IS] resilience plan”. On the other hand according to Type 2 technical oriented decision makers, “technology changes fast but from a technical perspective we see a pattern and what we do not know exactly is the detail of implementation but [we] can certainly do long term planning”. This justifies why the Type 1 decision makers rated it low whereas the Type 2 decision makers rated it high, which could not be predicted by Weill’s (2004) IT governance framework. Aligning Information Systems (IS) strategies with the strategic plan of the organisation” (rank 10) and “Adapting technology to strategic change” (rank 16). The first two statements fall under Weill’s (2004) IT infrastructure category while the last two fall under the IT architecture category, and hence are more technical than strategic. Lastly, Weill’s (2004) framework fails to predict statement number 22, which falls under both IT Principles and IT Infrastructure Strategies category. When probed Type 2 explained that, “It is about connectedness”, as illuminated by them, “we do not work in isolation, we are intermediaries between suppliers and our customers. It is crucial to ensure that we are connected hence it is important for us.” On the other hand, Type 1 again over estimates the independence of the firm to ensure resilience.

In this context an interesting finding related to factor analysis is worth mentioning. PRILO 3, a senior executive at Jade has demonstrated traits of both technical focused and



strategic focused decision makers. In fact he has a factor score of 0.5286 for type 1 and a factor score of 0.5397 for type 2 (see table 3). During interview we explored this slim difference in depth and indeed he has shown characteristics and qualities of both type of decision makers while prioritising his decisions. But his role within the organisation was technical and he also categorised himself under the technical category. So, we put him under type 2 (Technical focused decision maker).

### ***Consensus between Types 1 and 2***

Despite differences it is worth mentioning that there is a high correlation score (0.6018) between two types. This suggests that they are more in common than differences and as a result working as a team rather than as individuals. Providing reliable and consistent services to customers, capability for disaster recovery, setting up information disaster recovery system, resilient and accessible critical facilities and top management support and commitment to Information Systems (IS) resilience, which are critical to ensure IS resilience are prioritised highly by both types. These statements are critical to both types. The analytical procedure reports a list of “consensus statements”, for which both Types 1 and 2 are in agreement. Related to IS resilience planning we found that both types are in favour of both “flexible and adaptable” and “well defined and structured” plans. This was neither predicted by Agency Theory nor by IT governance framework. Moreover, the statements are paradoxical in nature. We probed, and found that Jade uses a hybrid approach when it comes to IS resilience planning. Following the Christchurch earthquakes in 2010 and 2011 the committee has reviewed IS resilience plans and the most significant conclusion drawn from review was that the plans should move from a rigid hierarchy which were focused on recovering from an ‘event based’ model to a more flexible ‘service recovery model’, which is neither scenario nor event specific. The service recovery

model identifies critical services, relates them to business need and specifies both service owners and consumers. This allows for a greater degree of flexibility in responding to different events and maintaining service-recovery documentation and process and ensures accountability. Some plans are well documented and structured, especially the DR, BC, Continuity of operations and Crisis Communication plans but some documents such as generic BCM Event Response Plan are flexible and adaptable. It outlines the high-level actions and decision-making process required in a BCM event. It references more specific procedures contained in the BCM portfolio. The objectives and activities this document describes are to be carried out by senior and line management staff during and immediately following a BCM Event to safeguard the immediate interests of, and minimise damage to, staff and customers.

### 5.1 Theoretical Framework

It is clear that Jade is attempting to balance the contrasts between governance of profitability and governance for revenue growth and innovation. Jade operates on a federal governance design, so they can achieve both the synergies emphasised in centralised models and the autonomy allowed by more decentralised models. Their governing IT principles emphasise sharing and reuse of process, system, technology and data modules.

Decision Archetypes	IT Principles		IT Architecture		IT Infrastructure		Business Application Needs		IT Investments	
	Input	Decision	Input	Decision	Input	Decision	Input	Decision	Input	Decision
Business Monarchy		√								√
IT Monarchy			√	√	√	√				
Federal	√						√	√	√	

IT Duopoly										
Feudal										
Anarchy										

*Table 5. IT Governance of IS resilience at Jade Software Corporation*

Table 5 shows our view (confirmed by senior management) of Jade's IT governance of IS resilience, reflecting responsibility for both decisions and input to those decisions. The main drivers for Jade's Business Continuity and Resilience Program are the contractual requirements to provide continuous support for global products and the operation of the managed services providing outsourcing for companies all over the world. In addition, as a software development company, access to collaboration tools, development environments and office support systems is critical. Jade values collaboration and it is purposely led and integrated into the culture of the organization. Jade has a committee that is responsible for risk management and IS resilience planning. The committee consists mostly of members of the c-suite executive management team responsible for the various areas of the company. They work together to ensure that all prospective risks are identified, mitigated, and planned for.

An important aspect of organisational resilience is IS resilience. Thus, agile and successful IS resilience planning requires a subset of organisational capabilities. As learnt from Jade, essential components of successful IS resilience planning can be summarised as:

***Sincere Top Management Commitment to Resilience:*** a vital requirement to IS resilience planning is the commitment at top management level and to reach effective IT governance, two-way communication and a good participation/collaboration relationship between the business and IT people are desirable. Adequate financial support to implement is also very important.

**Resilience Strategy:** clear strategy aligned to organisational goals and priorities must be formulated which has to be embedded in the organisation's culture.

**IS Resilience Planning Process and Implementation:** rather than a rigid hierarchy of plans derived from an 'event-based' model, it is critical to have a more flexible plan based "*service-recovery*", which is neither scenario based nor event specific. Agency Theory would ordinarily predict a less flexible plan, so as to transfer risk-bearing and decision rights away from employees at lower levels of the firm by creating more certainty about their duties. However, the context in which IS resilience plans are implemented are by definition highly uncertain, ambiguous, laden with risk, and require employees at all levels of the firm to act with greater degrees of autonomy and discretion so as to remain flexible in adverse circumstances or times of crisis. As highlighted by the senior executives, "In time of crisis plans go out of the window, it is important not to park those plans". This finding is not immediately obvious from the perspective of Agency Theory, but makes good sense in the unique context of IS resilience planning. In other words, there appears to be a special case of Agency Theory, when the plan is intended to be implemented in uncertain circumstances.

**Educating and Knowledge Sharing:** resilience includes learning and knowledge sharing, adaptation, innovation and staff training. Managers and employees need to be educated on a regular basis to create an organisation wide resilience culture. As identified by Kayes (2015), "It is the 'experienced' [person] who knows the limitations of all anticipation, the insecurity of all human plans. Experience teaches the incompleteness of all plans." This establishes a deep connection between resilience and learning, and points to a style of learning orientation that is closely aligned with resilience. It is also consistent with the findings about the need for a flexible plan, since training and education are necessary, if employees at all levels of the firm

will be expected to act with greater degrees of autonomy and discretion in times of crisis. In this case, therefore, training and education become a vehicle for the transference of risk-bearing and decision rights to employees at all levels of the firm.

***Continuous Testing and Monitoring:*** conducting dry-run or live test scenarios for testing specific service recovery strategies and regularly re-assessing risks and mitigation strategy. This finding also follows our finding about training and education, since it serves a purpose to enable employee preparedness at all levels of the firm.

***Regular and Transparent Communication:*** well-planned communication and change management is essential to effectively adapt to turbulent changes. This is consistent with the findings of the literature.

***Choose Your Partners Wisely:*** focus on key resilience attributes that really matter while choosing your partners is essential. This makes perfect sense, to ensure resilience it is important to safeguard your supply chain.

***Strong Understanding of Value Chain:*** important message is “connectedness”, value chain takes into consideration different types of inter organisational relationships, such as, suppliers, customers or the government.

***Collaborative Decision Making:*** When decision-making authority is delegated to agents, it cannot be guaranteed that the decisions will be aligned with the interest of the principal. However, when the principal has adequate information to verify agent behaviour, the agent is more likely to behave in favour of the principal (Eisenhardt, 1989). Senior executives at Jade make complex decisions in a collaborative manner. They interact as a team to select alternatives and prioritise objectives. They even experience the same consequences of the decision.

Depending on the problem scenario different members of the decision making team are responsible either individually or jointly for the different decisions. Senior executives at Jade exhibit all tenets of collaborative group decision making as identified by Keeney (Keeney, 2009). Importantly, the individuals involved in the decision making process may not prioritise the objectives in the similar way. Agency theory predicts this and emphasises the importance of monitoring agent behaviour. Collaborative decision making can be used as a device to monitor the behaviour of the agents and hence as a result principals may expect that agents will behave in favour of the principal. Moreover, as highlighted by several executives during the interview, due to the complexity of the business environment it is practically impossible for any one individual to make all aspects of decision making.

***Managing Uncertainty:*** As mentioned earlier in the literature review, Simon (1997) observed that most organisations try very hard to eliminate uncertainty because it is inefficient and hard to predict. As a result the majority of organisations try to plan for the unplannable. In Jade we observed that decision makers are quite comfortable with embracing risks. It reminds us of the fact that without uncertainty there is no innovation. Innovation is embedded at Jade which reflects in their decision making and management of uncertainty. Agency theory predicts that higher levels of uncertainty will be associated with higher levels of delegation of decision rights to the agent. Senior executives at Jade demonstrate some of the fundamental characteristics of risk embracing culture. First of all, senior executives at Jade are not afraid to take risks in the time of crisis. Prospect theory predicts that people adopt different decision behaviours under loss and gain domain. In other words, individuals seek risk in loss domain. During our interview we asked the senior executives to answer the risk preference related questionnaire and decision makers at Jade exhibit behaviours consistent with Prospect theory. Secondly, we

have not observed any sign of intense supervisions (Micromanagement) and higher levels of internal control at Jade (Red Tape). In other words, we have not found any evidence which may suggest Jade as a highly formalised, bureaucratic organisation. Lastly, senior executives at Jade are clear about the tasks they have to perform, mission of the organisation and goals they have to achieve. Clear communication related to goals, tasks and mission may encourage risk embracing culture. As the decision makers are likely to embrace risks in order to achieve organisational goals and mission.

Importantly, as identified in this research effective resilience planning should have the support of top management and address a variety of crisis scenarios. Organisations should regularly test, review and update the plan as needed, making sure everyone can perform their roles and responsibilities correctly. As predicted in the literatures, organisational culture towards embracing risk and managing and making decisions under uncertainty plays a vital role.

## **5.2 Strategy-Implementation Bi-cycle**

Jade's IS resilience committee is made up of members from both business and technical divisions. As identified before, both types are more similar than they are different. Members has clearly defined roles to ensure IS resilience at Jade. Business focused strategists work in a high and conceptual level predominantly dealing with the IT principles and IT investment and prioritisation type decision makings, whereas, technical focused tactical decision makers deal with the IT architecture and IT infrastructure related decision-making and both type play an important role to make decisions related to business application needs. This split between strategy and implementation is very crucial for Jade to make the right decisions which can be explained through "*Strategy-Implementation*" bi-cycle. This bi-cycle model will

be helpful to visualise at a high and conceptual level the split and relationship between the strategy and implementation cycle.

As shown in figure 6, the business focused decision makers are more associated with the strategy cycle and the technology focused decision makers are more associated with the implementation cycle. The IS resilience committee based on the business/IT strategy drives the definition and application of the IT governance principles and priority rules. Based on the service level agreements (SLAs) they then define the critical services. The Committee identifies the critical services and relates them to business needs and specifies both service owners and consumers to impose accountability and ensure smooth and uninterrupted delivery of services. The approved critical services are managed in the strategy cycle. After a decision has been made, critical services need to be implemented so they become part of the implementation cycle. These decisions are then implemented and monitored in the implementation cycle. As a result of continuous evaluation, critical services may continue without any changes or may need to be innovated and re-enter the strategy cycle through a new critical service. This helps decision makers at Jade to identify the critical services early, evaluate different options to address them and implement a solution.

As illustrated during interviews, “key risks are identified and understood and then we deal with them [risks].” Another executive stated, “we identify the key services first and then walk backwards to facilitate those services. This way a transformation happens from ‘passionate drive from individuals’ to ‘service critical thinking’.” The momentum generated due to this bi-cycle model in decision-making shows that IS resilience plans are never parked at Jade but are living documents. This has been described and emphasised eloquently by several committee members: “In time of crisis plans go out of the window, it is important not to park



those plans”; “Planning is critical but continual review is important.”; “We had a plan and people knew what to do [during events of crisis].”

Finally, the bi-cycle model clearly shows that quality of decision-making may be improved iteratively as the decision makers are more cautious and consider potential adverse effects of decisions before finalising it. This also means that the decision-making will take more time as the process is slower. However, once a decision has been made because of the consideration already given, the implementation will be faster.

This strategy-implementation bi-cycle has been verified and validated with the senior executives at Jade. More importantly, this study has identified that the “Strategy-Implementation bi-cycle” at Jade is consistent with the concept of Weill’s IT governance framework. IT governance has been defined as the accountability framework for IT decisions to enable desirable behaviours (Weill & Ross, 2004) and is viewed as a key responsibility of top management (Van Grembergen, 2002). The design of an organization’s IT governance framework is recognized in the literature as involving key trade-off decisions. For example, when IT decision rights are exclusively allocated to an IT unit, there is a considerable risk that the business interests are not adequately considered, resulting in a lack of business/IT alignment (Van Grembergen, 2002). On the other hand, if IT decision rights are allocated to business units, reflections from a technical as well as an enterprise-wide perspective are not sufficiently addressed. Whereas, if there are representation from both units in the top decision making committee then there is a fair possibility that both voices will be heard of.

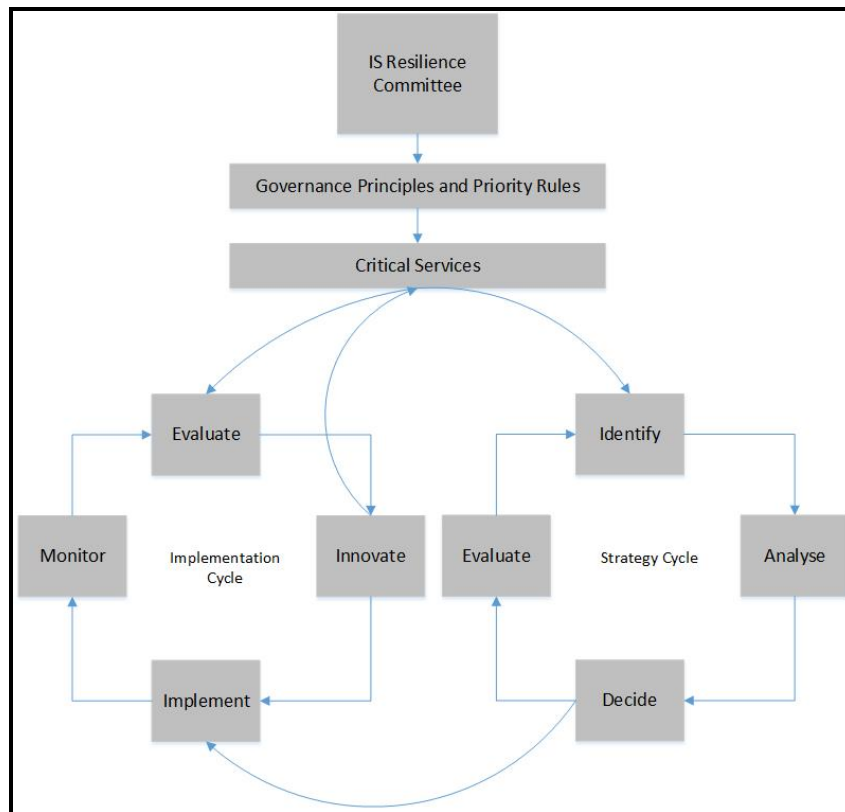


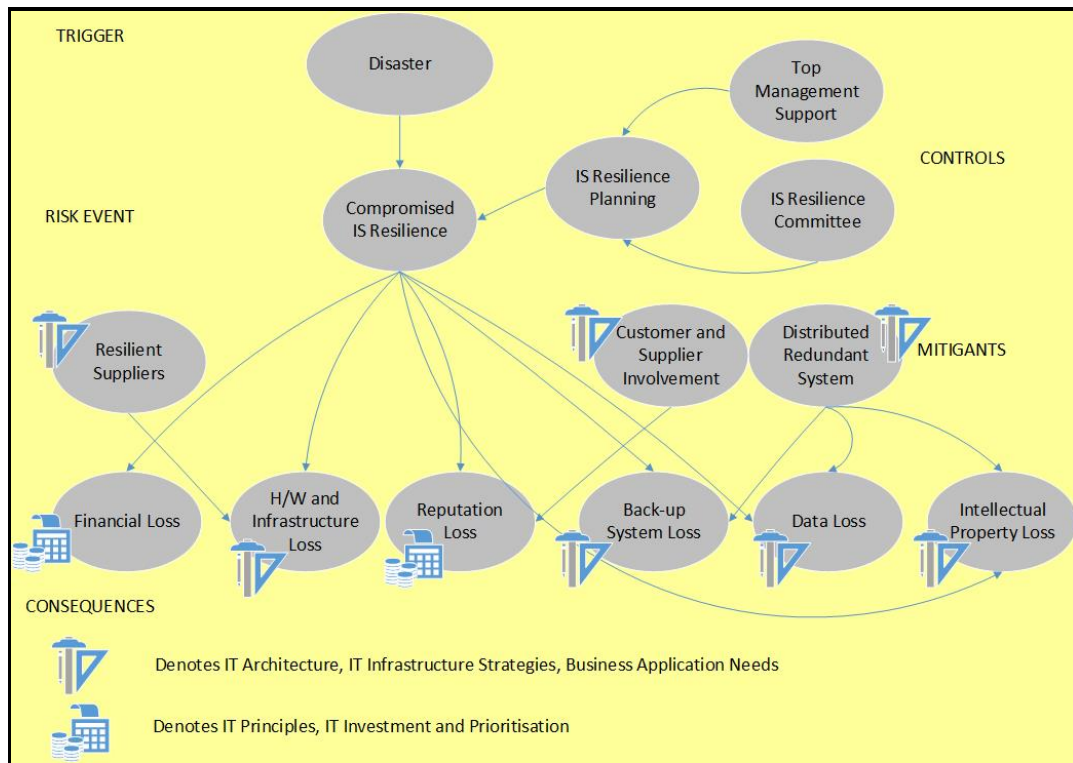
Figure 6. Strategy- Implementation “Bi-cycle” at Jade Software Corporation

### 5.3 How do senior executives make decisions

We will now take a causal perspective to explore the decision-making process of two different types of decision makers at Jade Software Corporation. The important message here is that the model combines various causal subjective and objective factors derived from careful reflection. In figure 4, we explained how to think rationally of IS resilience in terms of causal model with trigger events, control events, risk events, mitigate events and consequence events. Causal model has been used to explain how the decisions are made and responsibilities are shared by senior executives at Jade. This is a major contribution of our study as it explains the “gut-feel” decisions, which are based on doing all the reasoning “in the head” of the decision makers or relying on intuition. The causal model helps us to explore “*what lies under the bonnet*”. The causal model involves:

- The event itself
- At least one consequence event that characterises the impact
- One or more trigger events
- One or more control events which may stop the trigger event from causing the risk event
- One or more mitigating events which help avoid the consequence event

This is shown in figure 7. With this causal perspective, our risk event is “compromised IS resilience”, this event can be triggered by any form of disaster. The risk event also has a number of possible outcomes or consequences. Multiple controls can be put in place to avoid risk events and in case the risk event takes place then there are multiple mitigants that will reduce the impact of consequences. We found that the ability to decompose a IS resilience issue into chains of interrelated events should make decision-making more meaningful, rational, practical and coherent. The causal model clearly shows that the consequences can be divided into two types according to Weill’s IT governance framework, hence two types of decision maker in the TMT at Jade would complement each other to ensure IS resilience. As explained in the interview, *“IS resilience committee need wide spread knowledge, it is so complex that no one person understands it. We formed a collaborative team of members with different expertise. We have identified that not only having a plan is critical but execution of the plan is equally important”. As a collaborative effort committee first identified key risks. In order to derive those risks we looked at the service level agreements and customer contracts, then we have done a thorough business impact analysis, we have graded customer contracts and SLAs to address various business impacts.”*



*Figure 7. Causal Model for IS Resilience from the Decision Makers' Perspective at Jade Software Corporation*

This causal model has been verified with the senior executives at Jade and key lessons learnt from Jade are shared below:

**Structures:** the following quotes will help us to understand the IT governance structures in place at Jade. “We have plans, people knew what to do in time of crisis. Everyone has been trained and they have clearly defined roles and responsibilities.” And “we work together as a team. Organisations are dynamic and very complex. No one person understands all. The Right people doing the right thing is critical.” These quotes emphasise the importance of clearly defined roles and responsibilities and collective accountability. Delegating job to the right people and empowering staff was identified as critical in the interview. Another important factor was top management support, “it is absolutely critical to have support from the

board....top management creates culture.” Finally, there is an audit and compliance committee who has the specific responsibility for overseeing IT risks and monitoring IT priorities.

**Processes:** the following quotes will help us to understand the IT governance processes in place at Jade.

“We have detailed plans but the ability to planning is more important than the plan itself” and “it is important not to park those plans.” The emphasis is on IS resilience planning process. The senior executives has also mentioned that “continuous review of these plans is critical” and “capability to implement these plans is equally important”.

**Relational Mechanisms:** the following quotes will help us to understand the IT governance relational mechanisms in place at Jade. “Prepare your people so that they can respond”, “people should know what to do in a crisis”, “in times of crisis plans go out of the window...so empower staff so that they can be proactive to the recovery process.” Relational mechanisms are very important. It is possible that an organization has all the IT governance structures and processes in place, but it does not work out because business and IT do not understand each other and/or are not working together. Or, it may be that there is little business awareness on the part of IT or little IT appreciation from the business. So, to reach effective IT governance, two-way communication and a good participation/collaboration relationship between the business and IT people is needed. Ensuring ongoing knowledge sharing across departments and organisations is paramount for attaining and sustaining business/IT alignment. It is crucial to facilitate the sharing and the management of knowledge by using mechanisms such as career crossover (IT staff working in the business units and business people working in IT), continuous education, cross-training, etc.

#### **5.4 Necessary Elements of an IS Resilience Framework**

Our findings suggest that IT governance has significant influence for organisations when making decisions and assigning responsibilities and accountabilities. Though IS resilience frameworks are consistent with the existing IT governance framework, developed by Peter Weill (cites here) we have identified several unique attributes of IS resilience. This suggests that IS resilience planning is an instance of IT governance, however, it is distinct in several ways, and therefore justifies its own framework. For instance, IS resilience is unique because of the high degree of ambiguity and uncertainty.

IT governance suggests that implementation of processes, structures and relational mechanisms that enabled both IT and business managers to execute their roles and responsibilities in support of business-IT alignment will create value from IT-enabled investments, in other words, alignment of business and IT strategies improves business performance of an organisation. Figure 8 shows the necessary elements of IS resilience framework as derived from the findings of this research.

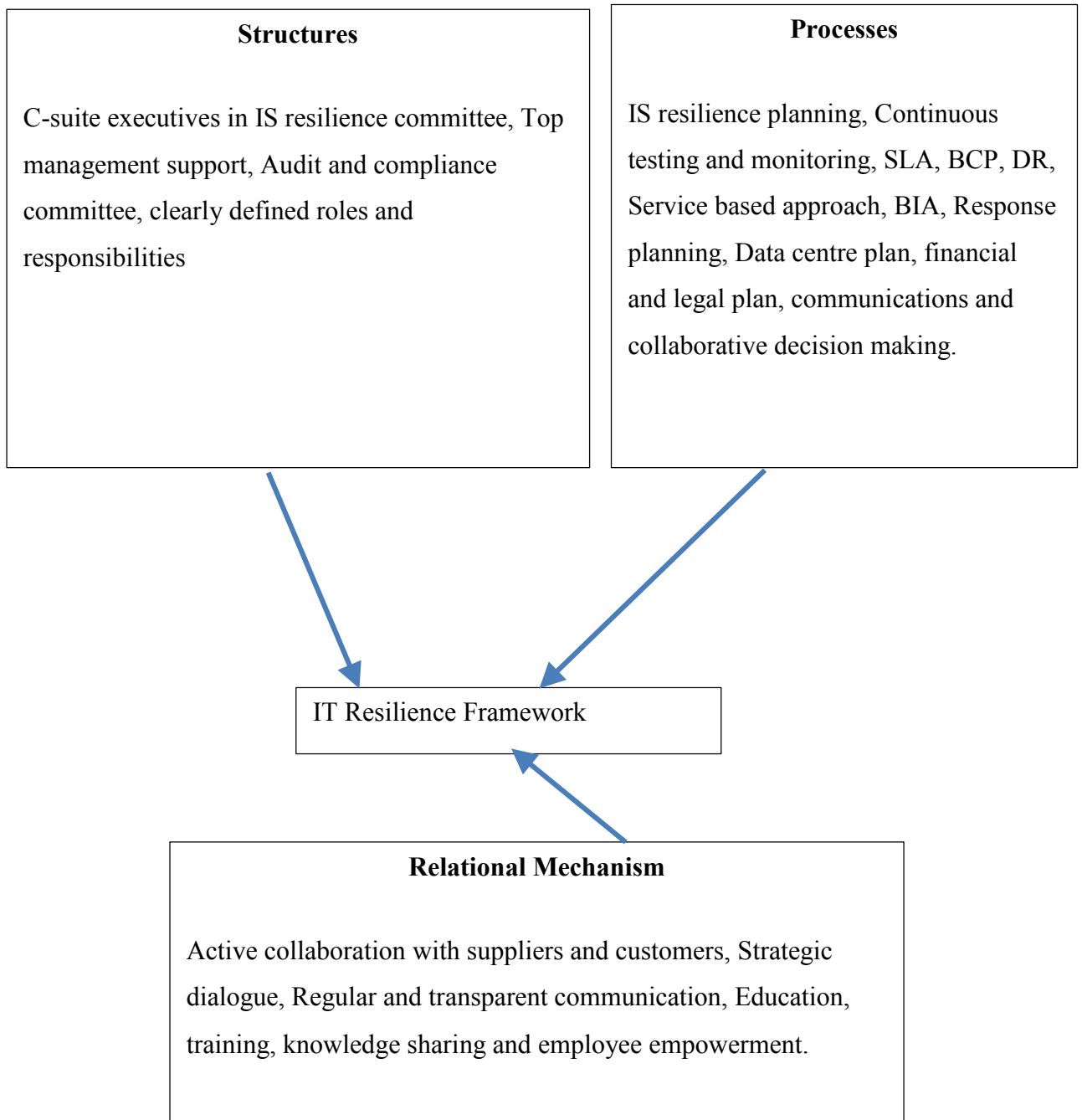


Figure 8. Necessary elements of IS Resilience framework.

## **6. CONCLUSION, CONTRIBUTION AND FUTURE RESEARCH**

An important aspect of IT governance and IS research is to describe phenomenon and explain their functions. In this study we have called attention to key descriptive aspects of top management team decision priorities in context of IS resilience and have identified two types of decision priorities within the top management team at Jade. We have emphasised the important distinctions as well as similarities among those types and types of information they convey. This rich, descriptive analysis was set in the functional IT governance framework, which is relevant to governance and decision-making in IS and we also viewed top managers' decision-making priorities through the theoretical lens of Agency Theory. Our contribution differs from any existing research in that it is rooted in two popular theories, namely, Agency Theory and IT governance framework. To best of our knowledge, this is the first attempt to build the concept of IS resilience separate from the concept of organisational resilience, and it appears to be valid. The types we have identified are complementary to each other and give us a more precisely characterised set of variables and important decision priorities in context to IS resilience framework to work with. This should be useful for academics and practitioners interested in decision priority and successful IS resilience planning.

The allocation of information technology (IT) decision rights between IT units and business units remains an important IT governance challenge. Companies that do not design an appropriate accountability framework for IT run the risk of business losses due to poor management decisions and misaligned IT priorities. While more detailed empirical work is necessary to elaborate and confirm the framework, it is believed that a useful starting point has been made. Understanding the decision-making by senior executives to ensure IS resilience informed us to develop an IS resilience framework that encompass IT governance structures,



processes and relational mechanisms. Effective IS resilience does not happen accidentally, rather requires thoughtful planning. We have described IS resilience planning in light of strategy-implementation bi-cycle and causal model is used to understand decision makers' perspective to understand decision priorities.

We identified a gap in existing research related to CIOs' and other key decision makers' decision-making priorities in context of IS resilience in organisations. We think that it is necessary to view the CIOs' and other key decision makers' decision-making priorities through the theoretical lens of Agency theory and Weill's IT governance framework. Accordingly, we conducted an extensive literature review to identify differences between private firms and public firms with respect to IS resilience and undertook an empirical study using Q-sort instrumentation to analyse key issues. Agency theory can be used to establish the decision priority differences between different types of organisations. Also Agency theory predicts that there will be decision priority differences between different types organisations. So our research study contributes to the limited body of knowledge on IS resilience in organisations in four ways. Firstly, our research shows that Agency theory is predictive to interpret decision priorities of CIOs and other key decision makers of organisations. Secondly, the concept that decision domains influence decision makers' decisions is a novel application of prospect theory that is not investigated in prior research. Thirdly, this is the first attempt to understand the IS resilience decision priorities of CIOs and key decision makers in lens of Agency Theory. Finally, by conducting an in depth study on the decision priorities of CIOs and other key decision makers in organisations we helped to identify the critical indicators of resilient organisations.

Main defining characteristic of decision-making is that it involves freedom of choice (Stephenson, 1973). Though choices are constrained but they exist within constraints—otherwise, no decision remains to be made. The exercise of choice reveals preferences, which are always subjective in the sense that from a decision maker's vantage point and one course of action is preferred over others, based on criteria with varying degrees of explicitness (Stephenson, 1973). Most decision-making scenarios are based on imperfect knowledge and thus no objectively right answer can be known in advance; hence, discretion is fundamental and impossible to remove (Stephenson, 1973).

Q methodology is referred to as “the best-developed paradigm for the investigation of human subjectivity” (Dryzek & Holmes, 2002). It provides a conceptual framework and systematic procedures for not only incorporating the participants' perspectives, but also placing them at the heart of analysis. It has much in common with qualitative methods (Watts and Stenner, 2012), but it is more rigorous at the point of data analysis.

Q methodology begins with decision makers' or stakeholders' thoughts and impressions typically expressed in their natural language on any topic that decision makers are called on to deliberate. Once gathered, the volumes of commentary comprising the concourse are reduced to a representative sample of assertions that participants use to represent their own individual views. The data are then correlated and the factors analysed, and the resulting factors point to the various perspectives at issue. The factors that emerge implicate genuine divisions among decision makers and stakeholders, and they reveal a basis of cooperation as well as sources of conflict. Therefore, Q methodology can contribute to the study of decision-making (i.e., to an understanding of why and how decisions are made) and can also assist in the

pragmatics of making decisions by providing information to decision makers about such things as the points of confluence and division among stakeholders.

The Q methodology does have some weaknesses. It is a small-sample technique, and the sample of items and participants is usually purposive, and the results lack generalizability. However, since the goals of Q-methodology are interpretive, this is usually not considered a weakness by Q-method practitioners. Another potential weakness is that the sample was restricted to Jade Software Corporation, hence the sample for this research is based in one location that is Christchurch, so it will not be possible to generalise the findings. Next, the survey conducted among the decision makers who are based in Christchurch, who have already experienced the problems mentioned in the scenario of the q study. This could differ to the decision priority of the persons who have not experience this particular scenario.

Our limitations also result some strengths. As this research is based in Christchurch it controls for the geographical as well as cultural variance. In future research we will gather data from different locations, within and outside New Zealand. For the next limitation, it would add realism to this study as all the key decision makers are able to reflect on their past experiences.

The study is a starting point for further research into the IS resilience in organisations. There are a number of avenues of future research, including examining a greater range of organisations. Future empirical research should attempt to understand the IS resilience decision priorities and characteristics of resilient organisations, both public and private, large and small. Another key research theme emerges from the study is, empirical research should attempt to understand the IS resilience decision priorities and characteristics of resilient organisations. Finally, results of this research will have implications both for researchers who

are looking for theories that explain the importance of IS resilience and business managers and owners who are challenged with decisions about how to design resilient information system framework for their organisation. This study contributes to the existing literature from both a theoretical viewpoint and a practical viewpoint.

## 8. REFERENCES

- Battisti, M., Lee, L., and Cameron, A. (2009). *Changing Business Focus-People, Planet and Profit : A Report of New Zealand SMEs and their Sustainability Practices*. Wellington, New Zealand: New Zealand Centre for Small and Medium Enterprise Reserach Massey University.
- Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International Journal of Production Research*, pp. 5375–5393.
- Blake, W. F. (1994). Making recovery a priority. *Security Management*, pp. 71-74.
- Bourgeois, L. J., & Eisenhardt, K. M. (1988). Strategic decision processes in high velocity environments: four cases in the microcomputer industry. *Management Science*, 816–835.
- Brown, S. R. (1980). *Political subjectivity: applications of Q Methodology in Political Science*. New Haven, CT: Yale University Press.
- Business Continuity Institute. (2012, Oct 28). *Good Practice Guideline*. Retrieved from Business Continuity Institute: [www.thebci.org](http://www.thebci.org)
- Cameron, A., & Massey, C. (2004). *Small and medium-sized enterprises: A New Zealand perspective*. Auckland, New Zealand: Pearson Education.
- Carr, N. (2003, May). IT Doesn't Matter. *Harvard Business Review*, pp. 1-17.
- Comfort, L. K. (2001). Complex systems in crisis: anticipation and resilience in dynamic environments. *Journal of Contingencies and Crisis Management*, pp. 144–158.
- Crichton, D. (2006). *Climate Change and Its Effects on Small Businesses in the UK*. London, UK: AXA Insurance.

Devlin, M. (1984). The Population of Small Businesses in New Zealand. Small Business Research Monographs, pp. 55-69.

Devraj, S., & Kohli, R. (2003). Performance Impacts of Information Technology: is actual usage the missing link? Management Science, pp. 273-289.

Dryzek, J. S., & Holmes, L. T. (2002). Post-communist Democratization. Cambridge, UK: Cambridge University Press.

Earl, M. J. (1993). Experiences in Strategic Information Systems Planning. MIS Quarterly, March, pp 1-27.

Effgen, K. F. (1992). Presenting the business case for a networked based disaster recovery planning program. Telecommunication, pp. 28-30.

Eisenhardt, K. M. (1989). Agency theory: an assessment and review. Academy of Management Review, pp. 57-74.

Fama, E. F., and Jensen, M. C. (1983). Separation of Ownership and Control. Journal of Law and Economics, pp. 1-30.

Fiedler, F. E. (1967). A theory of Leadership Effectiveness. New York, USA: McGraw Hill.

Gelinas, U. J., Dull, R. B., & Wheeler, P. R. (2012). Accounting Information Systems. Mason, USA: Cengage Learning.

Ghobadian, A., & O'Regan, N. (2006). The Impact of Ownership on Small Firm Behaviour and Performance. International Small Business Journal, pp. 555-586.

Gibb, F., & Buchanan, S. (2006). A Framework for business continuity management. *International Journal of Information Management* (26:2), pp.128-141.

Gibson, C & Tarrant, M. E (2010) A Conceptual Models Approach to Organisational Resilience, *Australian Journal of Emergency Management* 25 (2)

Goodwin, B. (2005, August 30). Business Continuity Spotlight falls on SMEs. *Computer Weekly*, p. 10.

Grover, V. (1990). Factors influencing adoption and implementation of customer based inter-organisational systems. Uni of Pittsburg.

Grover, V., Henry, R.M., & Thatcher, J.B. (2007). Fix IT-business relationships through better decision rights. *Communications of the ACM*, 50(12). pp. 80-86.

Gunasekaran, A., Griffin, M., & Rai, B. K. (2011). Resilience and competitiveness of small and medium size enterprises: an empirical research. *Journal of Production Research*, pp. 5489-5509.

Gurbaxani, V., & Whang, S. (1991). The impact of information systems on organizations and markets. *Communications of the ACM*, pp. 34-59.

Haes, S. D., & Grembergen, V., W. (2004). IT governance and its mechanisms. *Information Systems Control Journal*, 1(1), pp. 27-33.

Hann, J & Weber, R. (1996). Information Systems Planning: A Model and Empirical Tests," *Management Science* (42: 7), pp. 1043-1064.

Hatton, T., Seville, E., & Vargo, J. (2012). Improving the resilience of SMEs: policy and practice in New Zealand. Christchurch, New Zealand: Asia Pacific Economic Co-operation (APEC).

IBM. (2011). Key trends driving global business resilience and risk. IBM Global Technology Services.

Ingirige, B., & Wedawatta, G. (2011). Impacts of flood hazards on small and medium companies: strategies for property level protection and business continuity. *Flood Hazards, Impacts and Responses for the*, pp. 269-280.

Jensen, M. C., & Meckling, W. H. (1976, October). Theory of the firm : managerial behaviour, agency costs and ownership structure. *Journal of Financial Economics*, pp. 305-360.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decisions under risk.

Kayes, D.C. (2015). *Organisational Resilience: How Learning Sustains Organizations in Crisis, Disaster, and Breakdowns*, New York: Oxford University Press.

Keeney, R.L. (2009). The foundations of collaborative group decision. *International Journal of Collaborative Engineering*, Vol. 1, Nos. 1/2, pp.4–18.

Kim, B. G., & Lee, S. (2007). Factors affecting the implementation of electronic data interchange in Korea. *Computers in Human Behaviour*, pp. 1-21.

Klaus, Tim; Wingreen, Stephen C.; & Blanton, J. Ellis (2010). Resistant groups in enterprise system implementations: a Q-methodology examination. *Journal of Information Technology*, 25(1), pp. 91 – 106.



- Lee, C.K. & Wingreen, S.C. (2010). Transferability of knowledge, skills, and abilities along IT career paths: an Agency Theory perspective. *Journal of Organisational Computing and Electronic Commerce*, 20, pp. 23 – 44.
- Madni, A., M & Jackson, S (2009). Towards a Conceptual Framework for Resilience Engineering. *IEEE Systems Journal*, vol. 3, no. 2, pp. 181-191, June 2009.
- Massey, C. (2005). *Entrepreneurship and small business management in New Zealand*. Auckland: Pearson Education.
- Maurer, F & Lechner, U (2014). From Disaster Response Planning to e-Resilience: A Literature Review. *BLED 2014 Proceedings*. Paper 32. <http://aisel.aisnet.org/bled2014/32>.
- McManus, S., Seville, E., Vargo, J., & Brunsdon, D. (2008). Facilitated Process for Improving Organisational Resilience. *Natural Hazards Review*, pp. 81-90.
- Meade, P. (1993). Taking the risk out of disaster recovery services. *Risk Management*, 6-20.
- Ministry of Economic Development. (2012). *SMEs in New Zealand: Structure and Dynamics*. Wellington, New Zealand: Ministry of Economic Development.
- Muller, G., Koslowski, T., & Accorsi, R. (2013). Resilience – A New Research Filed in Business Information Systems. *ACM Symposium on Business Computing*, pp. 1-12.
- OECD. (2010). *SMEs, Entrepreneurship and Innovation*. Paris: Organisation for Economic Co-operation and Development.
- Paton, D. (2007). Measuring and Monitoring Resilience in Auckland. *GNS Science*, pp. 33-39.

Penn, Schohen, Berland. (2011). 2011 CRISIS PREPAREDNESS STUDY. Burson and Marsteller.

Penrose, J. M. (2000). The Role of Perception in Crisis Planning. *Public Relations Review*, pp. 155-165.

Poon, S., & Swatman, P. M. (1999). An exploratory study of small business Internet commerce issues. *Information and Management*, pp. 9–18.

Sayana, S. A. (2005). Auditing Business Continuity. *Information Systems Control Journal*, pp. 37-39.

Simon, H. A, (1997) *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization*. 4th ed. in 1997, The Free Press

Singleton, T. W. (2011). What Every IT Auditor Should Know About Backup and Recovery. *ISACA Journal*, pp. 1-2.

Smith, D. (1990). Beyond contingency planning: towards a model of crisis management. *Industrial Crisis Quarterly*, Elsevier Publishing, Vol. 4, pp. 263-275.

Snowden, D. J., & Boone, M. E. (2007). A leader's Framework for Decision Making. *Harvard Business Review*, 1-8.

Stephenson, W. (1973). Applications of Communication theory : III Intelligence and multi-valued choice. *Psychology Record*, 17-32.

Stephenson, W. (1986-1988). William James, Niels Bohr, and complementarity. *The Psychological Record*, vols 36-38

Stephenson, W. (1986a). Protoconcurus: The concourse theory of communication: I. Operant Subjectivity, Vol 9(2), Jan 1986. pp. 37-58.

Stephenson, W. (1986b). Protoconcurus: The concourse theory of communication: II. Operant Subjectivity, Vol 9(3), Apr 1986. pp. 73-96.

Storey, D. J. (1994). Understanding the Small Business Sector. London: Thomson Business Press.

Storey, D., & Greene, F. (2010). Small Business and Entrepreneurship. Harlow, UK: Pearsons Education.

Teoh, S. Y., & Zadeh, H. S. 2013. Strategic Resilience Management Model:Complex Enterprise Systems Upgrade Implementation. Pacific Asia Conference on Information Systems, pp. 88-95. Jeju Island, Korea: PACIS.

Thong, J. Y. (1999). An Integrated Model of Information Systems Adoption in Small Businesses. Journal of Management Information Systems, pp. 187-214.

Thun, H., Drüke, M., & Hoenig, D. (2011). Managing uncertainty – an empirical analysis of supply chain risk management in small and medium sized enterprises. International Journal of Production Research,pp. 5511-5525.

Vargo, J., & Seville, E. (2011). Crisis strategic planning for SMEs: finding the silver lining. International Journal of Production Research,pp. 5619-5635.

Vargo, J., & Stephenson, A. V. (2010). Measuring Organisational Resilience. World Conference on Disaster Management (pp. 44-51). Toronto, Canada: World Conference on Disaster Management.

- Vijayraman, B. S., & Ramakrishna, H. V. (1993). Disaster preparedness of small businesses with microcomputer based information systems. *Journal of Systems Management*, pp. 28-33.
- Watts, S & Stenner, P. (2012). *Doing Q methodological research: theory, method and interpretation*. London : Sage Publications.
- Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future : writing a literature review. *MISQ*, pp.1-26.
- Wedawatta, G., & Ingirige, B. (2012). Resilience and adaptation of small and medium-sized enterprises to flood risk. *Disaster Prevention and Management*, pp. 474-488.
- Weick, K. E., & Sutcliffe, K. M. (2007). Mindfulness and the quality of organisational attention. *Organization Science*, pp. 514-531.
- Wingreen, S.C., Blanton, J.E., Newton, S.K. & Domino, M. (2005) Assessing the IT training and development climate: an application of the Q-methodology. Atlanta, GA, USA: ACM SIGCPR/SIGMIS 2005 Computer Personnel Research Conference, 14-16 Apr 2005, pp. 12-23.
- Wingreen, S.C., LeRouge, C. & Blanton, J.E. (2009). Structuring Training for IT Professionals and the Firm: An application of the Q-methodology, *International Journal of Global Management Studies* 1(1): 53–67.
- Woodward, J. (1965). *Industrial Organisation : Theory and Practice*. New York, USA: Oxford University Press.

## 9. APPENDIX A

### Risk Orientation Questionnaire

As one of the top managers of my organisation ....	Strongly Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Strongly Agree
I believe that higher risks are worth taking for higher rewards.					
I accept occasional failures as being normal.					
I like to take big risks.					
I encourage the development of innovative strategies, knowing well that some will fail.					
I like to “play it safe.”					
I like to implement plans only if I am very certain that they will work.					
I prefer situations that have foreseeable outcomes.					
I avoid situations that have uncertain outcomes.					
I feel comfortable improvising in new situations.					
I avoid making decisions in uncertain situations.					

<b>I believe that greater risks are worth taking in a normal situation.</b>					
<b>I believe that greater risks are worth taking in an uncertain situation.</b>					
<b>Under normal circumstances, I encourage the development of innovative strategies, knowing well that some will fail.</b>					
<b>Under uncertain circumstances, I encourage the development of innovative strategies, knowing well that some will fail.</b>					
<b>I like to “play it safe” in a normal situation.</b>					
<b>I like to “play it safe” in an uncertain situation.</b>					

A. You have a choice between the following two options:

1. A sure gain of \$750.
2. 40% chance to gain \$2000 and 60% chance to gain nothing.

Please indicate which option you will choose.

B. You have a choice between the following two options:

1. A sure loss of \$1500.
2. 80% chance to lose \$2000 and 20% chance to lose nothing.

Please indicate which option you will choose.

C. You are offered the chance to buy the following gamble for \$3000:

50% chance of winning \$6000 and 50% chance of winning nothing.

Please indicate whether or not you will buy the gamble. **1=Yes 2=No**

Amitrajit Sarkar  
Department of Accounting & Information Systems  
University of Canterbury  
Telephone: +64 3 940 8495  
Email: [asa54@uclive.ac.nz](mailto:asa54@uclive.ac.nz)



## **Organisational Information Systems Resilience Consent Form for Information Systems Professionals**

I have been given a full explanation of this project and have had the opportunity to ask questions.

I understand what is required of me if I agree to take part in the research.

I understand that participation is voluntary and I may withdraw at any time without penalty. Withdrawal of participation will also include the withdrawal of any information I have provided should this remain practically achievable.

I understand that any information or opinions I provide will be kept confidential to the researcher and that any published or reported results will not identify the participants or their organisation.

I understand that all data collected for the study will be kept in locked and secure facilities and in password protected electronic form and will be destroyed after five years.

I understand the risks associated with taking part and how they will be managed.

I understand that I am able to receive a report on the findings of the study by contacting the researcher at the conclusion of the project.

I understand that I can contact the researcher, Amitrajit Sarkar ([Amitrajit.Sarkar@pg.canterbury.ac.nz](mailto:Amitrajit.Sarkar@pg.canterbury.ac.nz)) or supervisor, Dr. Stephen C. Wingreen ([stephen.wingreen@canterbury.ac.nz](mailto:stephen.wingreen@canterbury.ac.nz)) for further information. If I have any complaints, I can contact the Chair of the University of Canterbury Human Ethics Committee, Private Bag 4800, Christchurch ([human-ethics@canterbury.ac.nz](mailto:human-ethics@canterbury.ac.nz))

By signing below, I agree to participate in this research project.

Name: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

**Please return this completed consent form to Amitrajit Sarkar via email by 25/05/2015.**



Amitrajit Sarkar  
Department of Accounting & Information Systems  
University of Canterbury  
Telephone: +64 3 940 8495  
Email: [asa54@uclive.ac.nz](mailto:asa54@uclive.ac.nz)



## Organisational Information Systems Resilience Information Sheet for Information Systems Professionals

I am a post graduate researcher at Department of Accounting & Information Systems, University of Canterbury. You are invited to participate in the research project “Organisational Information Systems Resilience”.

The purpose of research is to gain a better understanding of the dynamics of the successful adaption of Information Systems (IS) within organisations and to understand the decision priorities of top managers in context to Information Systems Resilience.

Your involvement in this project will be to provide information about the decision priorities of Information Systems resilience planning by way of interview and each interview will take place at a time and venue convenient to you. A participant may be interviewed more than one time.

I would like to invite you to participate in my present study. If you agree to take part you will be asked to do the following:

Complete a questionnaire about the IS resilience decision priorities. In the questionnaire, you will be asked to rank a series of statements into order as well as explaining your reasoning behind the ranking. This will take approximately 20 to 25 minutes.

Please note that participation in this study is **voluntary**. If you do participate, you have the right to withdraw from the study at any time without penalty. If you withdraw, I will do my best to remove any information relating to you, provided this is practically achievable.

I will take particular care to ensure the **confidentiality** of all data gathered for this study. I will also take care to ensure your anonymity in publications of the findings. All the data will be securely stored in password protected facilities and in a secure place where only the researcher will have access for three years following the study. After that it will be purged. However, data with no identifying information will be securely stored for publication purposes in future.

The survey questionnaire is meant to be completed by the **person or persons responsible for managing IT/Information Systems in your firm**. All participants will receive a report on the study.

The research is being carried out by Amitrajit Sarkar ([Amitrajit.Sarkar@pg.canterbury.ac.nz](mailto:Amitrajit.Sarkar@pg.canterbury.ac.nz)) under the supervision of Dr. Stephen C. Wingreen ([stephen.wingreen@canterbury.ac.nz](mailto:stephen.wingreen@canterbury.ac.nz)). We will be pleased to discuss any concerns you may have about participation in the project.

This project has been reviewed and approved by the University of Canterbury Human Ethics Committee, and participants should address any complaints to The Chair, Human Ethics Committee, University of Canterbury, Private Bag 4800, Christchurch ([human-ethics@canterbury.ac.nz](mailto:human-ethics@canterbury.ac.nz)).

If you agree to participate in this study, please complete the **attached consent form** and return it to me via **email by 25/05/2015** along with the **completed questionnaire**. By participating you will gain feedback on how well your firm is prepared and also will gain access to a range of very useful practices relating to the effective management of Information Systems (IS). I am looking forward to working with you and thank you in advance for your contributions.

Yours Sincerely

Amitrajit Sarkar

## Q-SAMPLE

*Please read the scenario and the Q-sort technique before entering the statement numbers.*

Let us imagine a **scenario**, such as:

“Your business has been interrupted by a major incident. You have no access to your premises, IT systems and business records. Some of your employees are injured or dead. You do not know how long the outage is going to last. If you are *trying to plan ahead*, anticipating this scenario, what would your priorities be?”

### Q-sort distribution:

Keeping in mind the above scenario, rate which statements are important according to your experience *during Information Systems Resilience planning*. Assign the statements "from the outside in", that is, decide on two "very important" and "very unimportant" statements first, then select *four* statements each for the "important" and "unimportant" categories, and *six* statements each for "somewhat important" and "somewhat unimportant". The last *thirteen* statements need not be sorted, and will be categorized as "neutral". Enter the number to the left of each statement in the spaces provided. Please ensure that you enter a statement only once for each set of priorities.

Very Important (2 items)						
Important (4 items)						
Somewhat important (6 items)						
Somewhat unimportant (6 items)						
Unimportant (4 items)						
Very Unimportant (2 items)						

### General Information

1. Please indicate the total number of full-time and part-time employee in your firm.
  - Full Time .....
  - Part Time .....
2. What is your job title .....

1. s

**Key Issues for Each IT Decision Area (by Peter Weill)**

**IT Principles** ■ How do the business principles translate to IT principles that guide IT decision making?

- What is the role of IT in the business?
- What are desirable IT behaviours?
- How will IT be funded?

**IT Architecture** ■ What are the core business processes of the enterprise? How are they related?

- What information drives these core processes? How must this data be integrated?
- What technical capabilities should be standardized enterprise wide to support IT efficiencies and facilitate process standardization and integration?
- What activities must be standardized enterprise wide to support data integration?
- What technology choices will guide the enterprise's approach to IT initiatives?

**IT Infrastructure Strategies**

- What infrastructure services are most critical to achieving the enterprise's strategic objectives?
- What infrastructure services should be implemented enterprise wide and what are the service-level requirements of those services?
- How should infrastructure services be priced?
- What is the plan for keeping underlying technologies up-to-date?
- What infrastructure services should be outsourced?

**Business Application Needs**

- What are the market and business process opportunities for new business applications?
- How are strategic experiments designed to assess success?
- How can business needs be addressed within architectural standards? When does a business need justify an exception to a standard?
- Who will own the outcomes of each project and institute organisational changes to ensure the value?

**IT Investment and Prioritization**

- What process changes or enhancements are strategically most important to the enterprise?
- What is the distribution in the current IT portfolio? Is this portfolio consistent with the enterprise's strategic objectives?
- What is the relative importance of enterprise wide versus business unit investments? Do actual investment practices reflect their relative importance?
- How is the business value of IT projects determined following their implementation?

**Kindly identify, each statement falls under which IT Domain.**

Resilience Statements	IT Domain
-----------------------	-----------

1. Information Systems (IS) Disaster Recovery plans informed by understanding of underlying causes of vulnerability and other factors outside organisation's control.	
2. Organisation Information Systems (IS) Continuity plans, developed through participatory processes, put into operation and updated periodically.	
3. Organisation's Information Systems (IS) resilience plan shared with all suppliers.	
4. Organisation hazard/risk assessments carried out which provide comprehensive picture of all major hazards and risks faced by organisation (and potential risks).	
5. On-going monitoring of hazards and risks and updating of plans.	
6. Organisational vulnerability and capacity assessments carried out which provide comprehensive picture of vulnerabilities and capacities.	
7. Resilient and accessible critical facilities (e.g. back-up systems, redundancy of data).	
8. Top management support and commitment to Information Systems (IS) resilience.	
9. Information Systems (IS) resilience can provide an organisation with an edge over its competitors.	
10. Our competitors are developing and enhancing their Information Systems (IS) resilience capabilities.	
11. A sound Information Systems (IS) resilience plan will help us to win more business contracts.	
12. A sound Information Systems (IS) resilience plan will help us to pay lesser insurance premium.	
13. A sound Information Systems (IS) resilience plan will help our	

organisation to make more efficient use of resources.	
14. Long-term Information Systems (IS) Resilience, Business Continuity, Disaster recovery justification and planning.	
15. Competitor Analysis - Survive disruptions that your competitors cannot.	
16. Setting up information disaster recovery system (e.g., disk redundancy, backup facility).	
17. Study resilience strategies of competitors.	
18. Select suppliers with robust resilience plan.	
19. Use Information Systems (IS) network to communicate with the customers.	
20. Use Information Systems (IS) networks to connect to supplier's databases.	
21. Use cloud computing to back up organisational data.	
22. The level of customer involvement in preparing resilience, business continuity and disaster management plans.	
23. The extent of follow-up with customers for feedbacks.	
24. The level of supplier involvement in preparing resilience, business continuity and disaster management plans.	
25. Ensuring data security	
26. Receiving reliable and consistent services from Suppliers	
27. Providing reliable and consistent services to customers	
28. Capability for disaster recovery	

29. Providing the organisational units with information for 24 hours a day, 7 days a week	
30. Understanding the strategic priorities of top management	
31. Aligning Information Systems (IS) strategies with the strategic plan of the organization	
32. Adapting technology to strategic change	
33. Information Systems (IS) resilience plan that is well defined and structured	
34. Information Systems (IS) resilience plan that is flexible and adaptable	
35. Ability to identify key risks	
36. Ability to anticipate surprises and crises	
37. Committed, effective and accountable leadership of Information Systems (IS) resilience planning and implementation.	

**Distinguishing Statements for Types 1 and 2**

Resilience Statements	IT Decision Area (by Peter Weill)	Type 1		Type 2	
		<i>Q-SV</i>	<i>Z-SCR</i>	<i>Q-SV</i>	<i>Z-SCR</i>
2. Organisation ISCP plans, developed through participatory processes, put into operation and updated periodically.	IT Principles	2	1.46	1	0.63
3. Organisation's IS resilience plan shared with all suppliers.	IT Principles	0	-0.00*	-2	-1.23
4. Organisation hazard/risk assessments carried out which provide comprehensive picture of all major hazards and risks faced by organisation (and potential risks).	IT investments and priorities, IT Infrastructure Strategies	3	2.14*	1	0.86
6. Organisational vulnerability and capacity assessments carried out which provide comprehensive picture of vulnerabilities and capacities.	IT Investment and Prioritisation	2	1.47*	-1	-0.82
7. Resilient and accessible critical facilities (e.g. back-up systems, redundancy of data).	IT Architecture and Infrastructure Strategies	2	1.59	3	2.32
9. IS resilience can provide an organisation with an edge over its competitors	IT Principles	0	-0.26*	-2	-1.2
10. Our competitors are developing and enhancing their IS resilience capabilities	IT Principles	-2	-1.20	0	-0.41
14. Long-term IS Resilience, Business Continuity, Disaster recovery justification and planning	IT Infrastructure and IT Investment and Priority	-2	-1.22*	2	1.14
18. Select suppliers with robust resilience plan	IT Infrastructure Strategies	-1	-0.52*	2	1.00
22. The level of customer involvement in preparing resilience, business continuity and disaster management plans	IT Principles and IT Infrastructure Strategies	-2	-1.15*	0	0.23
31. Aligning IS strategies with the strategic plan of the organization.	IT Architecture	0	-0.26*	1	0.82
32. Adapting technology to strategic change.	IT Architecture	-2	-1.34*	0	0.14